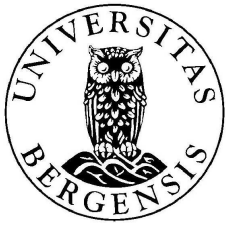
Noen sammenhenger mellom grafer, matroider, lineære koder og trelliser

Einar Kvale

Masteroppgave i
algebra



Matematisk Institutt
Universitetet i Bergen
Norge

11. april 2008

Fremfor alt må jeg få rette en stor takk til min veileder Trygve Johnsen for hans faglige og personlig motiverende veiledning gjennom oppgaveskrivingen. Han presenterte temaene oppgaven omhandler på en veldig oversiktlig måte og hans råd var helt avgjørende for hvilke retninger oppgaven tok.

Innledning

Denne masteroppgaven består i å finne sammenhenger mellom lineære koder, matroider og grafer. Gjennomgående for oppgaven er at vi presenterer kodeteoretiske konsept for så å formulere analogene til disse for matroider og deretter for grafer. Da en matroide, først introdusert av Whitney i 1935, er en abstrakt generalisering av en matrise, kan vi danne en matroide av en generatormatrise til en lineær kode. En matroide kan også ses på som en generalisering av en graf. Gitt en graf kan vi alltid danne en matroide. Matroider utgjør derfor det naturlige midtpunktet for lineære koder, matroider og grafer.
For linære koder i $(F_q)^n$ er det tre parametre som har vært av interesse for kodeteoretikere, kodelengden, n, dimensjonen k(antall informasjonsymboler i et kodeord) og minimumsdistansen, d. Gitt at vi ønsker å sende en informasjonsstreng på k biter over en usikker kanal, koder vi denne strengen ved at vi tilfører den $n-k$ biter, slik at eventuelle feil som oppstår under sending kan detekteres og/eller korrigeres. Minimumsavstanden er av interesse da denne angir hvor mange feil, t, en kode kan korrigere($t = \lfloor d - 1/2 \rfloor$). I [Wei] generaliseres minimumsavatanden til en følge med k elementer, $d_1, ..., d_k$, kalt de høyere vektene til koden. Det er ikke så intuitivt opplagt hva de høyere vektene, foruten d_1 som svarer til den tradisjonelle minimumsavstanden, representerer. Men de har fortolkninger i visse kryptologiske skjemaer, som vi ser på i kapittel 3. I tillegg viser det seg at de høyere vektene er av betydning ved å studere kompleksiteten ved trellisdekoding, som vi ser på i kapittel 6.
En lineær kode har en underliggende struktur som en matroide. Ved å la indeksmengden for kolonnene til generatormatrisen utgjøre grunnmengden til matroiden og de uavhengige mengdene av kolonner svare til de uavhengige mengdene til matroiden har vi en matroidestruktur. Alternativt kunne vi også danne en matroidestruktur ved å benytte en paritetssjekkmatrise til koden(en paritetssjekkmatrise og en generatormatrise gir gjensidig opphav til hverandre). Vi kan da definere alle parameterne $(n, k, d_1, ...d_k)$ via matroidestrukturen, og kan videre definere dem for matroider generelt. Som tidligere nevnt består mye av oppgaven i å formulere kjente egenskaper for koder i matroidespråk. Men alle egenskaper ved koder er ikke bestemt ved matroidestrukturen, og eksempler på dette er relativ dimensjon/lengde profil som vi ser på i kapittel 5. Heller ikke trellisdekoding som vi ser på i kapittel 6 er bestemt av matroidestrukturen.
Videre ser vi på hvordan de i utgangspunktet kodeteoretiske parameterne $(n, k, d_1, ..., d_k)$ kan fortolkes når de via matroidestruktur settes inn i en helt annen sammenheng, som for grafer. Vi ser da at minimusmavstanden svarer til den minste sykelen til en graf(sykel svarer til en minimal avhengig mengde). Videre vil de høyere vektene d_j svare til minste mulige antall kanter i en undergraf som inneholder j sykler. Antall sykler totalt svarer til dimensjonen k.

Vi begynner oppgaven med å presentere grunnleggende teori for lineære koder, matroider og grafer som vi bruker senere i oppgaven. Kapittel 1 utgjør denne delen.
I Kapittel 2 definerer vi vekthierarkiet til matroider og grafer. Vekthierarkiet ligger egentlig i grunn da vi senere introduserer ekvivokasjon og dimensjon/lengde profil i henholdsvis Kapittel 3 og 4. Deretter definerer vi MDS-egenskapen for matroider og grafer og formulerer og beviser noen resultat for MDS-grafer

I Kapittel 3 ser vi på en kryptologisk situasjon. I artikkelen til Lou, Mitprant, Vinck og Chen ser de på ekvivokasjonen(minimum usikkerhet) ved at to sendere sender to krypterte vektorer med informasjon til mottaker. Vi begrenser denne situasjonen ved at vi kun tar for oss en sender. Deretter ser vi på sammenhengen mellom ekvivokasjonen og de høyere vektene. Vi skal se at disse er bestemt av hverandre. Videre ser vi på ekvivokasjonen til MDS, nær-MDS og nesten-MDS koder for så å definere MDS-defekten, som er et mål for hvor langt en lineær kode er fra å være MDS(og derfor ha maksimal ekvivokasjon). Vi ser også på hvordan ekvivokasjon henger sammen med h-MDS og singletondefekten til en lineær kode. Til slutt i kapittel 3 generaliserer vi den kryptologiske situasjonen vi introduserte i begynnelsen av kapittelet til å gjelde for to sendere(matrise i to deler) som beskrevet i artikkelen til [LMVC].
I Kapittel 4 ser vi først på projeksjoner og underkoder, før vi innfører dimensjon/lengde profil, DLP, for en lineær kode. Deretter definerer vi DLP for matroider og formulerer resultatene som gjaldt for koder i matroidespråk. Deretter ser vi på sammenhengen mellom ekvivokasjon og DLP. Til slutt fortolker vi ekvivokasjon og DLP for en graf.
I Kapittel 5 utvider vi begrepet DLP til relativ dimensjon/lengde profil(RDLP). Videre forsøker vi å definere en relativ rangfunksjon, da rangfunksjonen ikke er oppfylt i det relative tilfellet. Vi definerer så en kvasimatroide ved å bruke den relative rangfunksjonen og ved den definere en dual relativ rangfunksjon. Deretter formulerer vi deler av teorien for matroider i kvasimatroidespråk. Dette vil generalisere mye av teorien for matroider.
I Kapittel 6 tar oppgaven en ny vending, da vi introduserer trelliser. Vi beskriver først hva en trellis er og hvordan vi kan konstruere en minimal trellis. Videre ser vi på hvordan DLP kan brukes for å optimere størrelsen på trellisen. For å motivere bruken av trelliser ser vi til slutt på trellisedekoding.

Innhold

Kapittel 1

Bakgrunnsmateriale

1.1 Grafteori

Vi begynner med grunnleggende grafteori.

En graf G består av en ikke-tom mengde $V(G)$ med hjørner og en multimengde $E(G)$ med kanter, der hver kant er et uordnet par av hjørner. La $e \in E(G)$ og $e = \{u,v\}$, der $u,v \in V(G)$. Vi sier at u og v er nabohjørner og at e er insident med u og v. Hvis $e = \{u,u\}$ sier vi at e er en løkke. Hvis $e_1 = e_2 = \{u,v\}$ er to kanter insidente til samme par av hjørner sier vi at e_1 og e_2 er multiple(paralelle) kanter. En graf er enkel dersom den ikke inneholder noen løkker eller multiple kanter.

To grafer G og G' er isomorfe hvis det eksisterer en en-til-en korrespondanse mellom hjørnene i G og i G' slik at alle par av hjørner er nabohjørner i G hvis og bare hvis det korresponderende par av hjørner er nabohjørner i G'

En sti i en graf G er en følge $v_0e_1v_1e_2\cdots v_{k-1}e_kv_k$ der $v_0,v_1,...,v_k$ er distinkte hjørner i G og følgelig $e_0,e_1,...,e_k$ er distinkte kanter. En krets(sykel) er en lukket sti, dvs $v_0 = v_r$ og $e_r = v_{r-1}v_r \in E(G)$.

En kantmengde $F \subseteq E(G)$ er uavhengig hvis F ikke inneholder noen kretser.

En graf H er en delgraf til en graf G hvis $V(H) \subseteq V(G)$ og $E(H) \subseteq E(G)$. En graf er sammenhengende hvis alle par av hjørner er forbundet av sti. En maksimal sammenhengende delgraf av en graf G kalles en komponent til G.

En sammenhengende graf sies å være et tre dersom den ikke inneholder noen sykler. Et utspennende tre til en graf G er en delgraf T av G slik at T er et tre og $V(T) = V(G)$. Et utspennende tre til en graf inneholder $|V(G)| - 1$ kanter. En skog er en graf,G, der hver komponent til G er et tre. Så et tre er en sammenhengende skog.

La G være en graf og la $F \subseteq E(G)$. Grafen vi får ved å fjerne kantmengden F betegnes ved $G\backslash F$. Hvis antall komponenter økes ved å fjerne F kalles F en separerende kantmengde til G. En minimal separerende kantmengde kalles en kokrets. En kokrets bestående av en kant kalles en bro.

En viktig klasse av grafer er de komplette grafene, K_n. I en komplett graf er alle mulige par av hjørner forbundet med en kant.

En planar graf er en graf som kan tegnes i planet uten at noen kanter skjærer hverandre. En planar graf deler planet inn i et endelig antall regioner. La H være en plan tegning av en graf G. Den geometriske dualen H^* til H kan konstrueres på følgende måte:

1.For hver region R i H sett inn et hjørne $v_R \in V(H^*)$

2.La mengden av kanter som avgrenser regionene R og R‘ være $\{e_1,e_2,...,e_k\}$ Vi forbinder v_F og $v_{F‘}$ ved k kanter $e‘_1,e‘_2,...,e‘_k$, der $e‘_i$ krysser e_i men ingen andre kanter i G. Hvis vi har en kant e som ikke avgrenser to regioner, adderer vi en løkke e‘ som krysser e og ingen andre kanter i G eller G*.

En digraf er en graf der kantene er ordnede par av hjørner. Hvis $D = (V(D),E(D))$ er en digraf sier vi at $G = (V(G),E(G)$, der $V(G) = V(D)$ og $E(G)$ er de uordnede elementene til $E(D)$, er den underliggende grafen til D. Vi kaller D for en orientering av G.

1.2 Matroider

Vi begynner med å definere en matroide.

Definisjon 1.2.1. *En matroide, M, er et par (E, I) der E er en endelig mengde og I er en familie av delmengder til E som oppfyller følgende egenskaper:*

i) $\emptyset \in I$

ii) Hvis $X \in I$ og $Y \subseteq X$, da vil $Y \in I$

iii) Hvis $X,Y \in I$ og $|X| < |Y|$, så eksisterer det $e \in Y - X$ slik at $X \cup e \in I$

Vi sier at E er grunnmengden til matroiden. Mengdene i I kalles uavhengige mengder. Komplementmengdene til mengdene i I med hensyn på E kalles de avhengige mengdene til matroidene.

En maksimal uavhengig mengde kalles en basis. Det er lett å vise at alle basismengdene har lik kardinalitet. Det er tilstrekkelig å definere en matroide ved å angi mengden av basiser, noe som følgende Teorem bekrefter:

Teorem 1.2.2. *La E være en mengde. En ikke-tom familie av delmengder β av E utgjør mengden av basiser til en matroide på E hvis og bare hvis β tilfredstiller følgende egenskap: Hvis B_1 og $B_2 \in \beta$ og $x \in B_1 - B_2$, så eksisterer $y \in B_2 - B_1$ slik at $(B_1 \cup \{y\}) - \{x\} \in \beta$*

Bevis. Se [Wel] □

En minimal avhengig mengde kalles en krets. En matroide er entydig bestemt ved å angi dens kretser. Dette gir opphav til en alternativ Definisjon av en matroide:

Teorem 1.2.3. *En matroide er et par (E, C), der E er grunnmengden og C er en familie av kretser slik at :*

i) $\emptyset \in C$

ii) Hvis C_1,$C_2 \in C$ *og* $C_1 \subseteq C_2$, *så er* $C_1 = C_2$

iii) Hvis C_1, $C_2 \in C$ *og* $e \in C_1 \cap C_2$, *så eksisterer det* $C_3 \in C$ *slik at* $C_3 \subseteq (C_1 \cup C_2)$ - $\{e\}$

Bevis. i) og ii) er trivielle. For bevis av iii) se [O]. □

Det finnes en måte å definere en matroide på som bruker rangfunksjonen til en matroide. Først definerer vi rangfunksjonen.

Definisjon 1.2.4. *La $M = (E, I)$ være en matroide. La $T \subseteq E$. Rangfunksjonen på M er funksjonen $r : 2^E \longrightarrow N \cup \{0\}$ definert ved:*

$$r(T) = max\{|X| \ |X \subseteq T \text{ og } X \in I\}$$

Vi kaller $r(T)$ rangen til T.

Rangen til matroiden M er da kardinaliteten til en maksimal uavhengig mengde.

Proposisjon 1.2.5. *La $M = (E, I)$ være en matroide. La $T \subseteq E$. Da har vi:*

i) T er uavhengig hvis og bare hvis $|T| = r(T)$

ii) T er en base hvis og bare hvis $|T| = r(T) = r(M)$

Bevis. Se [O].

□

Teorem 1.2.6. *En matroide består av en grunnmengde E og en funksjon r: $2^E \longrightarrow N \cup \{0\}$ slik at:*

i) $0 \leq r(X) \leq X$, for alle $X \subseteq E$

ii) Hvis $X \subseteq Y \subseteq E$, så er $r(X) \leq r(Y)$

iii) Hvis $X, Y \subseteq E$, så er $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$

Bevis. Se [Wil] □

Gitt at vi starter med en grunnmengde, E, og en rangfunksjon, r, vil de uavhengige mengdene i matroiden svare til de delmengder, T av E som oppfyller $|\mathrm{T}| = r(T)$. Det er derfor lett å se at rangaksiomene er ekvivalente med aksiomene gitt i Definisjon 1.2.1

Vi gir så et alternativt sett med aksiomer som er ekvivalente med aksiomene gitt i Teorem 1.2.6.

Teorem 1.2.7. *Gitt en grunnmengde E. En funksjon $r : 2^E \longrightarrow N \cup \{0\}$ er en rangfunksjon på E hvis og bare hvis følgende aksiomer er oppfylt for alle $X \subseteq E$, $x, y \in E$:*

i)' $r(\emptyset) = 0$

ii)' $r(X) \leq r(X \cup \{x\}) \leq r(X) + 1$

iii)' Hvis $r(X \cup \{x\}) = r(X \cup \{y\}) = r(X)$*, så vil* $r(X \cup \{x\} \cup \{y\}) = r(X)$

Bevis. Se [Wel] □

Eksempel 1.2.8. *Kanskje de enkleste eksemplene på matroider er de uniforme matroidene, $U_{k,n}$. Grunnmengden består av en n-mengde og mengden av basiser består av alle k-delmengder. Rangen til $U_{k,n}$ er k.*

En annen viktig klasse av matroider er de vektorielle matroidene. Følgende resultat viser hvordan vi kan konstruere en vektormatroide gitt en matrise.

Proposisjon 1.2.9. *La mengden E svare til kolonneindeksene til en $m \times n$ matrise A over en kropp K. La I være familien av delmengder X av E slik at de korresponderende multimengder av kolonneindekser i X er lineært uavhegig i vektorrommet K^m. Da er paret (E, I) en matroide, som kalles vektormatroiden til A og betegnes $M[A]$.*

Bevis. Se [O] □

En stor del av matroideteorien omhandler dualitet av matroider. Gitt en matroide kan vi alltid konstruere dens duale ved følgende resultat:

Teorem 1.2.10. *La M være en matroide og la $\beta(M)$ være mengden av basiselementer til M. Da vil $\beta^*(M) = \{E(M) - \beta | B \in \beta(M)\}$ være mengden av basiser til M^* på grunnmengden $E(M)$.*

Vi kaller M^* den duale matroiden til M.

En viktig bemerkning er at i motsetning til en graf, som kan ha flere ulike dualiseringer, har en matroide en unik dual. Ved å dualisere den duale matroiden er det lett å se at $(M^*)^* = M$. Vi sier at en basis i M^* er en kobasis i M. Tilsvarende er en krets i M^* en kokrets i M

Eksempel 1.2.11. *Den duale til den uniforme matroiden $U_{k,n}$ er gitt ved: $U^*_{k,n} = U_{n-k,n}$.*

Det er lett å se at dersom r^* betegner rangfunksjonen til M^* så har vi: $r^*(M) + r(M) = |E(M)|$. Vi gjengir følgende resultat fra [O] som viser sammenhengen mellom rangfunksjonen til M og den duale rangfunksjonen til M(dvs rangfunksjonen til M^*).

Proposisjon 1.2.12. *La M være en matroide på grunnmengden E. La $X \subseteq E$. Da vil:*

$$r^*(X) = |X| + r(E - X) - r(E)$$

Bevis. Se [O] □

Vi definerer nå to matroideoperasjoner kalt sletting og kontraksjon:

Definisjon 1.2.13. *La $M = (E, I)$ være en matroide. La $T \subseteq E$.*

i) Matroiden $M \setminus T = (E - T, I(M \setminus T))$, der $I(M \setminus T) = \{X \subseteq E - T | X \in I(M)\}$ kalles slettingen av T fra E.

ii) Matroiden $M/T = (M^* \setminus T)^*$ på grunnmengden $E - T$ kalles kontraksjonen av T fra M

Definisjon 1.2.14. *La $M_1 = (E_1, I_1)$ og $M_2 = (E_2, I_2)$ være to matroider. Vi sier at M_1 og M_2 er isomorfe, betegnet ved $M_1 \cong M_2$, hvis det eksisterer en bijeksjon $\varphi : E_1 \longrightarrow E_2$ slik at $X \in I_1$ hvis og bare hvis $\varphi(X) \in I_2$, for alle $X \subseteq E_1$*

Vi kunne også definert matroideisomorfi ved at det må eksistere en kretsbevarende eller rangbevarende bijeksjon mellom E_1 og E_2.

Gitt en graf $G = (V,E)$. Vi kan konstruere en matroide, M, fra grafen G ved å la kantmengden E(G) svare til grunnmengden i M og syklene i G svare til kretsene i M. Vi kaller matroiden $M(G) = (E(G),C)$ kretsmatroiden til G. Vi har her brukt den alternative Definisjonen fra Teorem 1.2.3 istedenfor Definisjon 1.2.1

Eksempel 1.2.15. *Kretsmatroiden til K_3 er isomorf med den uniforme matroiden $U_{2,3}$*

1.3 Kodeteori

Vi betegner vektorrommet av dimensjon n over F_q som $(F_q)^n$

Definisjon 1.3.1. *En blokk-kode, C, er en undermengde av $(F_q)^n$*

Definisjon 1.3.2. *En kode C er en lineær kode hvis C er et underrom av $(F_q)^n$*

Dersom C er et k-dimensjonalt underrom av $(F_q)^n$ sier vi at C er en lineær [n,k]-kode. Lengden til kodeordene er n. Av disse vil k av elementene være informasjonssymboler. Det er disse som utgjør informasjonen i kodeordene. De siste $n-k$ elementene kalles sjekksymboler og har som funksjon å detektere og/eller korrigere feil ved sending over usikre kanaler. Vi kaller $r = n-k$ redundansen til koden.

Definisjon 1.3.3. *La $\underline{x}$ og $\underline{y}$ være to kodeord(vektorer) i C. Hammingavstanden $d_H(\underline{x}, \underline{y})$ er lik antall posisjoner der $\underline{x}$ og $\underline{y}$ er forskjellige. Dvs:*

$$d_H(\underline{x}, \underline{y}) = |\{i | x_i \neq y_i, i = 1, ..., n\}|$$

Definisjon 1.3.4. *Minimumsavstanden, d, til C er den minste Hammingavstanden mellom alle mulige par av kodeord. Dvs:*

$$d = min_H\{(\underline{x}, \underline{y}) | \underline{x}, \underline{y} \in C, \underline{x} \neq \underline{y}\}$$

Definisjon 1.3.5. *Hammingvekten $w(\underline{x})$ til en kode C er antall koordinater forskjellig fra null:*

$$w(\underline{x}) = |\{i | x_i \neq 0, i = 1, ..., n\}| = d(\underline{x}, \underline{0})$$

Definisjon 1.3.6. *Mininumsvekten $w(C)$ til en kode C er den minste vekten forskjellig fra null:*

$$w(C) = min\{w(\underline{c}) | \underline{c} \in C - \{\underline{0}\}\}$$

Det er vanlig å betegne en blokk-kode C for en (n, M, d)-kode, der n er lengden, M er antall kodeord og d er minimumsavstanden. En lineær kode betegnes som en $[n, k, d]$-kode, der k er dimensjonen til koden. Antall kodeord er q^k.

Teorem 1.3.7. *La C være en lineær kode. Da vil minimumsvekten til C være lik minimumsavstanden til C:*

$$d(C) = w(C)$$

Bevis. Se [H] □

Teorem 1.3.8. *(Singletonbegrensningen): For en (n, M, d)-kode har vi at:*

$$M \leq q^{n-k+1}$$

Bevis. Se [H] □

For en lineær kode er det vanlig å angi Singletonbegrensningen som en øvre begrensning av d: $d \leq n-k+1$.

Da en lineær kode er et underrom er det nok å spesifisere C ved en basis. For en $[n,k]$-kode C danner vi en $k \times n$ matrise, G, der radene i matrisen utgjør en basis til C. En slik G kalles en generatormatrise til C. Alle kodeordene i C kan uttrykkes som en lineærkombinasjon av radene i G.

Vi definerer nå ekvivalens for koder, og formulerer deretter et viktig resultat som viser hvordan vi kan omforme en generatormatrise på noe som kalles standard form.

Definisjon 1.3.9. *Vi sier at to lineære koder C_1 og C_2 er ekvivalente dersom den ene koden kan fås fra den andre ved å permutere koordinatene til koden(dvs ved å permutere kolonneindeksene til generatormatrisen) og/eller ved å multiplisere koordinatene(kolonnene) med skalarer forskjellig fra null.*

Teorem 1.3.10. *La G være en generatormatrise for en $[n,k]$-kode C. Ved å utføre elementære rad og kolonneoperasjoner kan vi omforme G på standard form $[I_k \ B]$, der I_k er $k \times k$ identitetsmatrise og B er en $(n-k) \times k$ matrise.*

Bevis. Se [H] □

En $(n-k) \times n$ matrise, H, med rang $n-k$ som oppfyller $GH^T = [0]$ kalles en paritetssjekkmatrise til C. En vektor $\underline{c}$ er et kodeord hvis og bare hvis $\underline{c}H^T = \underline{0}$.

Teorem 1.3.11. *La C være en $[n,k]$-kode. La $G = [I_k \ B]$ være generatormatrisen på stanard form. Da er en paritetssjekkmatrise, H, gitt ved $H = [-B^T \ I_{n-k}]$.*

Bevis. Se [H] □

Definisjon 1.3.12. *Dualkoden til C er gitt ved mengden av vektorer som er ortogonale med alle kodeordene i C:*

$$C^{\perp} = \{x \in (F_q)^n | \underline{xc} = 0, \forall \underline{c} \in C\}$$

Teorem 1.3.13. *La $G = [I_k \ B]$ være generatormatrisen til en $[n,k]$-kode C. Da er $C^{\perp}$ en $[n, n-k]$-kode med en generatormatrise $H = [-B^T \ I_{n-k}]$, og G er en paritetssjekkmatrise til $C^{\perp}$.*

Bevis. Se [H] □

Vi har definert minimumsavstanden, d, til en kode. Vi skal nå definere en generalisering av denne. Først definerer vi støtten og støttevekten til en kode

Definisjon 1.3.14. *La C være en $[n,k]$-kode og D en underkode. Støtten $\chi(D)$ er mengden av alle posisjoner der ikke alle vektorer er null:*

$$\chi(C) = \{i : (x_1, x_2, ..., x_n) \in C, x_i \neq 0)\}$$

Definisjon 1.3.15. *Støttevekten er kardinaliteten til* $\chi(C)$

Definisjon 1.3.16. *Den r-te generaliserte Hammingvekten til C,* $d_r(C)$*, er den minste støttevekten til en r-dimensjonal underkode:*

$$d_r(C) = min\{|\chi(D)| \mid D \text{ er en underkode av rang } r\}$$

Vi kaller $d_1(C), ..., d_k(C)$ de høyere vektene til C. Vi har at $d_1(C)$ er den tradisjonelle minimumsavstanden til C.

Definisjon 1.3.17. *Vekthierarkiet til C er gitt ved:*

$$\{d_r(C)|1 \leq r \leq k\}$$

De høyere vektene oppfyller en streng monotoniegenskap som neste resultat viser.

Teorem 1.3.18. *For en* $[n, k]$*-kode C har vi:*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n$$

Bevis. Se [Wei] □

Singletonbegrensningen for lineære koder sier at $d \leq n-k+1$. Neste resultat generaliserer singletonbegrensningen.

Korollar 1.3.19. *For en* $[n, k]$*-kode har vi:*

$$d_r(C) \leq n - k + r$$

Teorem 1.3.20. *La H være en paritetssjekkmatrise for en kode C. La* $<H_i|i \in I>$ *være kolonnerommet utspent av kolonnevektorne* H_i*. Da har vi:*

$$d_r(C) = min\{|X| : |X| - rang(< H_i|i \in I >) \geq r\}$$

Bevis. Se [Wei] □

Den generaliserte Hammingvekten $d_r(C)$ er lik d hvis og bare hvis det eksisterer kolonner i H slik at rommet som utspennes har rang høyst $d-h$, og det ikke eksisterer $d-1-h$ kolonner som spenner ut et rom av dimensjon $\leq d-1-h$. For en kode C vil minimumsavstanden $d(C)$ være lik d hvis og bare hvis det eksisterer d kolonner i H slik at rangen til kolonnerommet er $d-1$, og det ikke eksisterer $d-1$ kolonner slik at rommet som utspennes er av dimensjon $\leq d-2$.

Det er en sterk sammenheng mellom de høyere vektene til C og $C^{\perp}$.

Teorem 1.3.21. *La C være en* $[n, k]$*-kode. Da vil:*

$$\{d_r(C)|1 \leq r \leq k\} \cup \{n + 1 - d_r(C^{\perp})|1 \leq r \leq n - k\} = \{1, 2, ..., n\}$$

Bevis. Se [Wei] □

Vi har tidligere definert singletonbegrensningen for lineære koder. Vi definerer nå koder som oppfyller denne begrensningen med likhet.

Definisjon 1.3.22. *En $[n, k, d]$-kode er en MDS kode hvis $d = n - k + 1$*

Definisjon 1.3.23. *La C være $[n, k, d]$-kode. Singletondefekten til C er gitt ved:*

$$S(C) = n - k + 1 - d$$

Merk at C er en MDS kode hvis og bare hvis $S(C) = 0$. Vi definerer så lineære koder som ikke oppfyller singletonbegrensningen men som nesten gjør det.

Definisjon 1.3.24. *C er nesten-MDS hvis $S(C) = 1$*

Definisjon 1.3.25. *C er nær-MDS hvis $S(C) = S(C^\perp) = 1$*

Raddum ser på i [R] hvordan vi kan beskrive MDS, nesten-MDS og nær-MDS ved de høyere vektene for en kode C. La C være MDS. Vi har at $d_1 = n-k+1$. Derfor vil ingen av tallene $n+1-d_r(C^\perp)$ stå blant tallene $d_1(C), ..., d_k(C)$, da vi hadde fått $d_1 < n-k+1$. Setter vi opp tallene $\{d_r(C)|1 \leq r \leq k\} \cup \{n+1-d_r(C^\perp)|1 \leq r \leq n-k\} = \{1, 2, ..., n\}$ i stigende rekkefølge får vi sekvensen:

$$n+1-d_{n-k}(C^\perp), ..., n+1-d_1(C^\perp), d_1(C), ..., d_k(C)$$

Dersom C er nesten-MDS vil $d_1 = n-k$. Da vil et av tallene $n+1-d_i^\perp$ stå blant $d_1(C), ..., d_k(C)$. Setter vi opp tallene ${}_r(C)|1 \leq r \leq k\} \cup \{n+1-d_r(C^\perp)|1 \leq r \leq n-k\} = \{1, 2, ..., n\}$ i stigende rekkefølge vil sekvensen bli:

$$n+1-d_{n-k}(C^\perp), ..., n+1-d_2(C^\perp), d_1(C), ..., d_i(C), ..., n+1-d_1^\perp(C), d_{i+1}, ..., d_k$$

Dersom C er nær-MDS vil $d_1(C) = n-k$ og $d_1(C^\perp) = n-(n-k) = k$. Da vil $n+1-d_{1(C^\perp)} = n-k+1$. Så $n+1-d_1(C^\perp)$ vil stå på plassen etter $d_1(C) = n-k$. Sekvensen blir derfor:

$$n+1-d_{n-k}(C^\perp), ..., n+1-d_2(C^\perp), d_1(C), n+1-d_1(C^\perp), d_2(C), ..., d_k(C)$$

Definisjon 1.3.26. *En h-MDS kode er en kode der h er det minste tallet slik at $d_h = n-k+h$*

For $h = 1$ svarer dette til den tradisjonelle minimumsavstanden, så en MDS-kode er 1-MDS. Dersom $d_h = n-k+h$ så vil $d_i = n-k+i$ for $h < i \leq k$

Vi har følgende resultat:

Proposisjon 1.3.27. *C er nær-MDS hvis og bare hvis C og $C^{\perp}$ begge er 2-MDS.*

Proposisjon 1.3.28. *C er nær-MDS hvis og bare hvis C er nesten-MDS og 2-MDS.*

Bevis. Se [R] □

Vi avslutter denne seksjonen med et Eksempel som oppsummererer mye av teorien vi har gjennomgått.

Eksempel 1.3.29. *Betrakt den lineære koden C med parametre $[n, k, d] = [7, 4, 3]$. En generatormatrise på standard form, $G = [I_4, B]$ er gitt ved:*

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Av Teorem 1.3.11 er en paritetsjekkmatrise, $H = [B^T, I_3]$, gitt ved:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Av Teorem 1.3.13 er H en generatormatrise til dualkoden til C

Ved å liste opp alle kodeordene til $C^{\perp}$ er det lett å se at den minste vekten til et ikke-null kodeord er 4. Av Teorem 1.3.8 vil da $d(C^{\perp}) = 4$. Singletondefekten til C og $C^{\perp}$ er gitt ved henholdsvis: $S(C) = n - k - d + 1 = 7 - 4 - 3 + 1 = 1$, $S(C^{\perp}) = 7 - 3 - 4 + 1 = 1$. Da $S(C) = S(C^{\perp}) = 1$ vil C være nær-MDS. (Av Proposisjon 1.3.27 har vi også at C og $C^{\perp}$ er 2-MDS). Da C er nær-MDS og $d_1(C) = 3$ vil de høyere vektene være gitt ved:

$$d_1(C) = 3,\ d_2(C) = 5,\ d_3(C) = 6,\ d_4(C) = 7$$

De høyere vektene til $C^{\perp}$ er gitt ved:

$$d_1(C^{\perp}) = 4,\ d_2(C^{\perp}) = 6,\ d_3(C^{\perp}) = 7$$

Svaret er i overenstemmelse med at:

$$\{d_h(C) | 1 \leq d_h(C) \leq 4\} \cup \{n + 1 - d_h(C^{\perp}) | 1 \leq d_h(C^{\perp}) \leq 3\} = \{1, 2, 3, 4, 5, 6, 7\}$$

Kapittel 2

Noen sammenhenger mellom matroider, grafer og koder

2.1 Vekthierarkiet til matroider og grafer

Gitt en $[n, k]$-kode C kan vi konstruere vektorielle matroider svarende til generatormatrisen G og paritetssjekkmatrisen H.

Definisjon 2.1.1. *La C være en $[n, k]$-kode med generatormatrise G. La $M[G]$ være en vektormatroide av rang k på indeksmengden $\{1, 2, ..., n\}$ for kolonnene til G. Da sier vi at $M[G]$ er vektormatroiden til C.*

Vi sier at M[G] er matroiden som korresponderer til C. Vi kan også betegne denne matroiden som M_C.

Vi vet at hvis C er en $[n, k]$-kode med paritetssjekkmatrise, H, vil H være generatormatrisen til $C^{\perp}$. Følgende resultat viser hvordan vi kan konstruere vektormatroiden $M[H]$ som korresponderer til $C^{\perp}$.

Proposisjon 2.1.2. *La M være matroiden som korresponderer til $[n, k]$-koden C. Da vil M^* korrespondere til $C^{\perp}$.*

Definisjon 2.1.3. *La M være en matroide på grunnmengden E. La $T \subseteq E$. Den h-te høyere vekten til M er definert ved:*

$$d_h(M) = min\{|T| \ /r(T) = |T| - h\}$$

Definisjon 2.1.4. *Vekthierarkiet til M er definert ved:*

$$\{d_h(M)|1 \leq h \leq n - r\},$$

der r er rangen til matroiden

Vi formulerer så matroideanalogen til Teorem 1.3.21:

Proposisjon 2.1.5. *La M være en matroide med rang r. Da vil:*

$$\{d_h(M)|1 \leq h \leq n-r\} \cup \{n+1-d_h(M^{\perp})|1 \leq h \leq r\} = \{1,2,...,n\}$$

Bemerkning 2.1.6. *Dette resultatet med lignende bevis ble gitt som Proposisjon 5.8 i [L]*

Bevis. La $F(T)$ og $F^*(T)$ være to funksjoner gitt ved:

$$F(T) = |T| - r(T),\ F^*(T) = |T| - r^*(T)$$

La videre $h(x)$ og $h^*(x)$ være gitt ved:

$$h(x) = max\{F(T) \mid |T| = x\},\ h^*(x) = max\{F^*(T) \mid |T| = x\}$$

Ved å bruke Proposisjon 1.2.11 har vi at:

$$F^*(T) = |T| - r^*(T) = |T| - |T| - r(E-T) + r(T) = r - r(E-T)$$

$$= r - |E-T| + |E-T| - r(E-T) = r - |E-T| + F(E-T)$$

Da vil:

$$max\{F^*(T) \mid |T| = x\} = r - n + x + max\{F(T)| \ |T| = n - x\}$$

som gir:

$$h^*(x) = r - n + x + h(n-x)$$

eller:

$$h^*(x) = h(x) + r - x$$

De høyere vektene er nå gitt ved:

$$d_1(M) = min\{|T| \mid |T| - r(T) = 1\} = min\{x|h(x) = 1\}$$

$$d_2(M) = min\{|T| \mid |T| - r(T) = 2\} = min\{x|h(x) = 2\}$$

$$\vdots$$

$$d_{n-r}(M) = min\{|T| \mid |T| - r(T) = n-r\} = min\{x|h(x) = n-r\}$$

Vi har da at d_i-ene er lik $\{x|h(x) - h(x-1) = 1\}$. Vi ser at d_i-ene gjør et sprang for hver i. For h^* har vi at:

$$h(x) - h(x-1) = h^*(n-x) - r + x - h^*(n-x+1) + r - x + 1$$

$$= h^*(n-x) - h^*((n+1)-x) + 1 = 1 - (h^*((n+1)-x) - h^*(n-x)$$

Vi har da at:

$$h(x) - h(x-1) = 1, \text{ hvis } d_i\text{-ene gjør et sprang. Og 0 ellers.}$$

Derfor vil:

$$h(x) - h(x-1) = 0 \iff (h^*((n+1) - x) - h^*(n-x)) = 1$$

Men da vil:

$$x = d_i, \text{ for passe } i \iff (n+1) - x \text{ ikke er en dualvekt, } d_j^*, \text{ for noen } j.$$

□

Bemerkning 2.1.7. *Hvis C er en kode med vekthierarki ${}_h(C)|1 \leq h \leq n-r\}$, og vektormatroidene $M[G]$ og $M[H]$ svarer til generatormatrisen og paritetssjekkmatrisen til C, vil $\{d_h(C)|1 \leq h \leq n-r\}$ svare til de høyere vektene til $M[H]$.*

Tilsvarende definerer vi de h-te høyere vektene for en graf G.

Definisjon 2.1.8. *La $G = (V, E)$ være en en graf. La $T \subseteq E$. Den h-te høyere vekten til G er definert ved:*

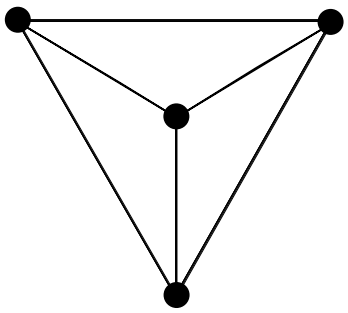
$$d_h(G) = min\{|T||r(T) = |T| - h\}$$

I definsjonen ovenfor er $r(T)$ definert via rangfunksjonen til matroiden $M[G]$.

Definisjon 2.1.9. *La $n = |E|$ og la r være rangen til grafen G. Vekthierarkiet er definert ved:*

$${}_h(G)|1 \leq h \leq n-r\}$$

Vi har da at $d_h(G)$ svarer til den minste undergrafen som inneholder h sykler. Ved å fjerne h kanter(en kant fra hver sykel) får vi et utspennende tre til undergrafen.



Figur 2.1: Den komplette grafen med fire hjørner

Eksempel 2.1.10. *Betrakt den komplette grafen K_4. Den minste sykelen inneholder 3 kanter. Derfor vil $d_1 = 3$. Ved å legge til to kanter får vi den minste undergrafen som inneholder 2 sykler. Da vil $d_2 = 5$. Videre vil $d_3 = 6$. Vekthierarkiet er gitt ved $\{3, 5, 6\}$.*

2.2 MDS-grafer og nær-MDS-grafer

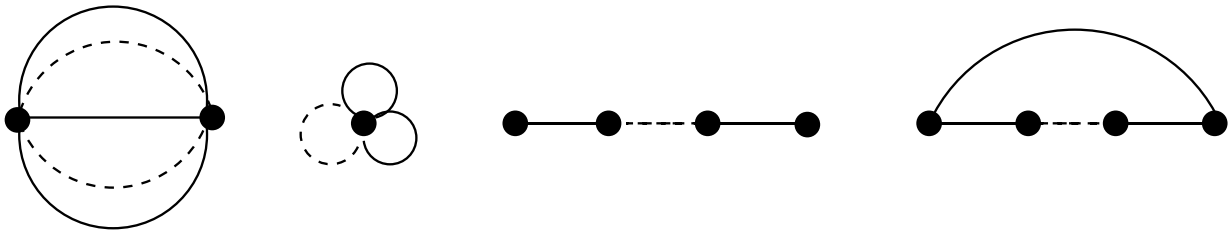
Vi ser nå på MDS-egenskapen for grafer.

Definisjon 2.2.1. *En graf $G = (V, E)$ er en MDS-graf hvis G er en skog eller $d = n-k+1$, der n er antall kanter, k er kardinaliteten til vekthierarkiet og $d = d_1$ svarer til antall kanter til den minste sykelen.*

Merk at rangen til grafen er gitt ved $r = n - k$.

Definisjon 2.2.2. *En graf G er en triviell MDS-graf hvis $k \in \{0, 1, n-1, n\}$*

Det er lett å vise at det eksisterer trivielle MDS-grafer. La $k = n$. Da vil G være grafen med et hjørne og n løkker. Da vil d_1 være lik 1. Singletondefekten blir $S(G) = n - k + 1 - d = n - n + 1 - 1 = 0$. La $k = n - 1$. Da vil G være grafen med to hjørner og $n - 1$ multiple kanter. Den minste sykelen i G vil inneholde 2 kanter. Dvs $d_1 = 2$. Da vil $S(G) = n - (n - 1) + 1 - 2 = 0$. La $k = 1$. Da vil $d_1 = n$ og $S(G) = n - 1 + 1 - n = 0$. La $k = 0$. Da er G et tre som per Definisjon er MDS. Figur 2.2 illustrerer strukturen til de trivielle MDS-grafene.



Figur 2.2: De trivielle MDS-grafene

Teorem 2.2.3. *Det eksisterer ingen ikke-trivielle MDS-grafer for $n \geq 4$.*

Bevis. Anta at G er en ikke-triviell MDS-graf for $n \geq 4$. Da G er ikke-triviell vil $k \in \{2, .., n-2\}$. Da vil $d_1 = n - k + 1 \geq n - (n-2) + 1 = 3$. Siden $k \geq 2$, vil G inneholde to sykler C_1 og C_2. La T være delgrafen bestemt av C_1 og C_2. Disse har eventuelt noen felles kanter, som kan ses på som "en rett linje" delt inn i a kanter. La C_1 være sykelen som består av kantene i a og en kantmengde a_1 slik at $C_1 = aa_1$. La C_2 være sykelen bestående av kantene i a og en kantmengde a_2 slik at $C_2 = aa_2$. Da vil også a_1a_2 være en sykel, dersom $a = 0$. Vi har nå at $d_1 \leq d_2 - 2$ (for en MDS-graf er de høyere vektene påfølgende) for en av syklene C_1, C_2 eller a_1a_2 ville ha fjernet minst to kanter fra T, siden minst to av stiene må lengde minst 2, da $d_1 \geq 3$. □

Korollar 2.2.4. *En undergraf til en MDS-graf er MDS*

Bevis. Ved å fjerne en kantmengde med k kanter fra grafen med et hjørne og n looper får vi en graf med et hjørne og $n - k$ kanter. Ved å fjerne k kanter fra grafen med to hjørner

$n-1$ multiple kanter får vi en graf med $n-k-1$ multiple kanter. Ved å fjerne k kanter fra en sykel får vi en skog med k komponenter. Ved å fjerne k kanter fra et tre får vi en skog med $k+1$ komponeneter. □

Vi definerer så nær-MDS egenskapen for grafer på samme måte som for koder.

Definisjon 2.2.5. *G er en triviell nær-MDS-graf hvis $k \in \{0, 1, n-1, n\}$ og $d_1 = n-k$ for G og G^*.*

Eksempel 2.2.6. *Det er lett å vise at det eksisterer ikke-trivielle nær-MDS-grafer for $n \leq 6$. Betrakt den komplette grafen K_4. Av Eksempel 4.8 vet vi at vekthierarkiet er gitt ved $\{3, 5, 6\}$. Da vil $n = 6$, $k = 3$ og $d_1 = 3$. Singletondefekten til K_4 er da $S(K_4) = n - k - d_1 + 1 = 1$. K_4 er selvdual så $S(K_4^*) = 1$*

Det kan vises at det ikke eksisterer ikke-trivielle nær-MDS grafer for n $\geq$ 7. Vi overlater det til leseren å bevise dette.

Kapittel 3

Ekvivokasjon ved kanalavlytting

3.1 "Wire-tap" kanal

Vi skal nå se på en kryptologisk situasjon. Vi beskriver først den kryptologiske problemstillingen, før vi ser hvordan dette henger sammen med matroide og kodeteorien vi har beskrevet tidligere i oppgaven.

En sender har r informasjonsbits $\mathbf{y} = [y_1, ..., y_r]^T$ han ønsker å sende til en mottaker. La A være en $r \times n$ matrise. Da sender ønsker å skjule informasjonen $\mathbf{y} = [y_1, ..., y_r]^T$ for avlyttere velger han en vektor $\mathbf{x} = [x_1, ..., x_n]^T \in F^n$ slik at $A\mathbf{x} = \mathbf{y}$. I kryptografiske termer er $\mathbf{x}$ nøkkelen og matrisen A offentlig. A er derfor kjent for potensielle avlyttere. Da $\mathbf{x}$ sendes vil en tredjepart kunne avlytte $x_{i1}, ..., x_{is}$. La $\sigma = \{i_1, ..., i_s\}$. La Z^σ være begivenheten at tredjeparten avlytter $\{x_i | i \in \sigma\}$. Før vi går videre definerer vi entropi.

Definisjon 3.1.1. *Entropien til en variabel Y er gitt ved:*

$$H(Y) = -\sum_{y \in (F_q)^r} p(y) log_q p(y)$$

Her er $(F_q)^r$ utfallsrommet og $p(y)$ sannsynligheten for at $Y = y$. Merk at fordi $p(y) \leq 1$ vil $log_q p(y) \leq 0$. Derfor vil $H(Y) \geq 0$. Entropien er et mål for usikkerheten i utfallet til Y. Dersom det ikke er noe usikkerhet i utfallet til Y vil $H(Y) = 0$. Jo større $H(Y)$ er, desto større usikkerhet vil det være.

Definisjon 3.1.2. *Vi definerer entropien til Y gitt at vi kjenner begivenheten Z^σ ved:*

$$H(Y|Z^\sigma) = -\sum_{y \in (F_q)^r} p(Y = y|Z^\sigma) log_q p(Y = y|Z^\sigma)$$

I vårt tilfelle vil $H(Y|Z^\sigma)$ være et mål for usikkerheten i Y gitt at en tredjepart kjenner $Z^\sigma = \{x_i | i \in \sigma\}$

Definisjon 3.1.3. *Minimum usikkerhet (også kalt ekvivokasjon) er definert ved:*

$$\triangle_s = minH(Y|Z^\sigma),\ \textit{der } \sigma \textit{ varierer over alle valg av delmengder av } \{1,...,n\} \textit{ med kardinalitet } s$$

Proposisjon 3.1.4. *La $A = [H_1, H_2, ..., H_n]$. Da vil $\triangle_s = minrang < H_i|i \notin \sigma >$, der σ varierer over alle valg av delmengder av $\{1,...,n\}$ med kardinalitet s*

Merk at hvis $s = 0$ vil $\sigma = \emptyset$. Da vil Δ_0 svare til rangen til matrisen A.

Bevis. Da $minH(Y|Z^\sigma)$ og $minrang < H_i|i \notin \sigma >$ varierer over de samme delmengder er det tilstrekkelig å vise at $H(Y|Z^\sigma) =$ rang $< H_i|i \notin \sigma >$. Anta, uten tap av generalitet, at $A = [B|C]$, der $\sigma = \{1, 2, ..., s\}$ utgjør kolonneindeksene til B og $S - \sigma = \{s+1, ..., n\}$ utgjør kolonneindeksene til C. Dersom tredjeparten avlytter $x_1, ..., x_s$ har vi at rang $< H_i|i \notin \sigma >= rangC$. Vi må derfor vise at $H(Y|Z^\sigma) = rangC$. Heretter lar vi Λ betegne $rangC$.

La Γ være løsningsmengdene for $(x_{s+1}, ..., x_n)$ av ligningen $A\mathbf{x} = \mathbf{y}$, for fast $\mathbf{y}$ og $x_1, ..., x_s$. Dvs $B[x_1, ..., x_s]^T + C[x_{s+1,...,x_n}]^T = \mathbf{y}$. Vi har at $x_1, ..., x_s$ er kjent for avlytter, så dette er en ligning i $n - s$ variabler. Vi kan omskrive dette til $C[x_{s+1,...,x_n}]^T = \mathbf{y} - B[x_1, ..., x_s]^T = [z_1, ..., z_r]$. Hvis $[z_1, ..., z_\Lambda] \notin Col(C)$, får vi ingen løsning for $(x_{s+1}, ..., x_n)$ så $\Gamma = \emptyset$ Hvis $[z_1, ..., z_r] \in Col(C)$, vil antall løsninger for $(x_{s+1}, ..., x_n)$ være gitt ved: $|\Gamma| = q^{n-s-\Lambda}$.

La $p(Y = \mathbf{i}|Z^\sigma)$ være sannsynligheten at Y tar verdien $\mathbf{i}$ gitt at vi kjenner $x_1, ..., x_s$, dvs:

$$p(Y = \mathbf{i}|Z^\sigma) = p(Y = \mathbf{i}|X_1 = x_1, ..., X_s = x_s).$$

Av Bayes Teorem kan dette uttrykkes ved:

$$\frac{p(X_1 = x_1, ..., X_s = x_s|Y = \mathbf{i})p(Y = \mathbf{i})}{p(X_1 = x_1, ..., X_s = x_s)} 1)$$

Da utfallsrommet $(F_q)^r$ for Y har q^r elementer vil sannsynligheten for at $Y = \mathbf{i}$ være gitt ved: $\frac{1}{q^r}$. Sannsynligheten for at $X_i = x_i$, der $i = 1, ..., s$ er gitt ved $\frac{1}{q}$. Sannsynligheten for at $X_i = x_i$, for $i = 1, ..., s$ er gitt ved produktet av sannsynligetene dvs. $\frac{1}{q^s}$. Vi kan nå uttrykke 1) som:

$$\frac{p(X_1 = x_1, ..., X_s = x_s)|Y = \mathbf{i})\frac{1}{q^r}}{\frac{1}{q^s}} 2)$$

Sannsynligheten $p(X_1 = x_1, ..., X_s = x_s|Y = \mathbf{i})$ kan uttrykkes som summen over alle sannsynligheter der $(x_{s+1}, ..., x_n) \in (F)^{n-s}$ varierer. Dersom $\Gamma = \emptyset$ vil denne summen bli 0. Dersom $\Gamma \neq 0$ kan 2) uttrykkes som

$$q^{s-r}(\sum_{x_{s+1},...x_n \in \Gamma} \frac{1}{q^{n-r}}) = q^{s-r-n+r+n-s-\Lambda} = q^{-\Lambda}$$

La $\mathbf{i}$ være slik at $(x_{s+1}, ..., x_n) \in \Gamma(\mathbf{i})$. Vi har nå at:

$$H(Y|Z^\sigma) = -\sum_i p(Y = \mathbf{i}|Z^\sigma) log_q p(Y = \mathbf{i}|Z^\sigma) = -\sum_i q^{-\Lambda} log_q q^{-\Lambda} = -\sum_i q^{-\Lambda}(-\Lambda) = \Lambda$$

Den siste likheten ovenfor følger av at summen av alle sannsynlighetene er 1.

□

3.2 Sammenheng mellom ekvivokasjon og høyere vekter

Vi ser nå på hvordan ekvivokasjon har sammenheng med de høyere vektene til en kode. La A være en paritetssjekkmatrise til en $[n, n-r]$-kode C. La $d_1(C), ..., d_k(C)$ være de høyere vektene til C. Av Teorem 1.3.20 vil $d_j(C)$ være bestemt av kolonnene til A ved:

$$d_j(C) = \min\{t | \exists t \text{ kolonner } H_{i,1}, ..., H_{j,t} \text{ av } A, \text{ slik at } \text{rang}[H_{i,1}, ..., H_{j,t}] \leq t - j\}$$

Følgende resultat viser hvordan ekvivokasjonen og de høyere vektene til en kode er bestemt av hverandre.

Proposisjon 3.2.1. *La Δ_s for $0 \leq s \leq n$ være ekvivokasjonen til kanalen med matrise A som beskrevet ovenfor. La C være en [n,k] kode med paritetssjekkmatrise A. Da vil: $\Delta_o = n - k$(rangen til A). For $1 \leq s \leq n$ er Δ_s gitt ved:*

$$d_{n-s-\Delta_s}(C) \leq n - s < d_{n-s-\Delta_s+1}(C),$$

hvor vi per konvensjon setter $d_0 = 0$

Vi gjengir følgende bevis fra [Wei]s artikkel med noen korreksjoner:

Bevis. Av prop. 3.1.4 vet vi at det eksisterer I, slik at $|I| = n - s$ og $\text{rang}(< H_i : i \in I >) = \Delta_s$. Vi har at $d_{n-s-\Delta_s}(C) \leq n - s$. Anta at $n - s \geq d_{n-s-\Delta_s+1}(C)$. Ved å bruke Teorem 3.1.4 igjen har vi at det eksisterer I slik at $|I| = d_{n-s-\Delta_s+1}(C) = n - s - \epsilon$, $\epsilon \geq 0$ og $\text{rang}(< H_i : i \in I >) = |I| - (n - s - \Delta_s + 1) = \Delta_s - \epsilon - 1 \leq \Delta_s - 1$. Men da vil $\Delta_s \leq \Delta_{s+\epsilon} \leq \Delta_s - 1$, som er en selvmotsigelse. Derfor vil $n - s < d_{n-s-\Delta_s+1}(C)$. □

Vi illustrerer denne Proposisjonen med et Eksempel:

Eksempel 3.2.2. *Betrakt Hammingkoden C med parametre $[15, 11]$. Vekthierarkiet er gitt ved: $\{3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15\}$. Vi har at $\Delta_0 = n - k = 15 - 11 = 4$. Videre vil Δ_s for $1 \leq s \leq n$ være gitt ved:*

$$d_{14-\Delta_1} \leq 14 < d_{15-\Delta_1} \Longrightarrow \Delta_1 = 4$$

$$d_{13-\Delta_2} \leq 13 < d_{14-\Delta_2} \Longrightarrow \Delta_2 = 4$$

$$d_{12-\Delta_3} \leq 12 < d_{13-\Delta_3} \Longrightarrow \Delta_3 = 4$$

$$d_{11-\Delta_4} \leq 11 < d_{12-\Delta_4} \Longrightarrow \Delta_4 = 4$$

$$d_{10-\Delta_5} \leq 10 < d_{11-\Delta_5} \Longrightarrow \Delta_5 = 4$$

$$d_{9-\Delta_6} \leq 9 < d_{10-\Delta_6} \Longrightarrow \Delta_6 = 4$$

$$d_{8-\Delta_7} \leq 8 < d_{9-\Delta_7} \Longrightarrow \Delta_7 = 4$$

$$d_{7-\Delta_8} \leq 7 < d_{8-\Delta_8} \Longrightarrow \Delta_8 = 3$$

$$d_{6-\Delta_9} \leq 6 < d_{7-\Delta_9} \Longrightarrow \Delta_9 = 3$$

$$d_{5-\Delta_{10}} \leq 5 < d_{6-\Delta_{10}} \Longrightarrow \Delta_{10} = 3$$

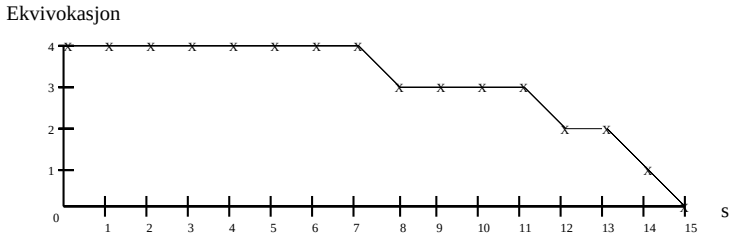
$$d_{4-\Delta_{11}} \leq 4 < d_{5-\Delta_{11}} \Longrightarrow \Delta_{11} = 3$$

$$d_{3-\Delta_{12}} \leq 3 < d_{4-\Delta_{12}} \Longrightarrow \Delta_{12} = 2$$

$$d_{2-\Delta_{13}} \leq 2 < d_{3-\Delta_{13}} \Longrightarrow \Delta_{13} = 2$$

$$d_{1-\Delta_{14}} \leq 1 < d_{2-\Delta_{14}} \Longrightarrow \Delta_{14} = 1$$

$$d_{0-\Delta_{15}} \leq 0 < d_{1-\Delta_{15}} \Longrightarrow \Delta_{15} = 0$$



Figur 3.1: Ekvivokasjonskurven til [15,11]-Hammingkoden

Bemerkning 3.2.3. *Av Figur 3 ser vi at fallene til ekvivokasjonskurven korresponderer til vekthierarkiet til* $C^{\perp}$*:* $\{8, 12, 14, 15\}$

Av grafen ser vi at $\Delta_s = 4$, for $0 \leq s \leq 7$. Det betyr at avlytter ikke får noe informasjon ved å avlytte de syv første bitene. Ved å få kjennskap til den åttende biten vil ekvivoksjonen avta. Deretter vil vil den avta ved avlytting av den 12-te,14-de og 15-de biten. Vi ser at $\Delta_{15} = 0$, da det ikke vil være noen usikkerhet hvis avlytter kjenner alle bitene.

I Eksempel 3.2.2 viste vi hvordan vi kan finne Δ_s gitt at vi kjenner de høyere vektene til C. Ved å reversere prosedyren kan vi finne de høyere vektene gitt at vi kjenner ekvivokasjonen. Vi har at mengden $\{s|\Delta_s = \Delta_{s+1}\}$ korresponderer til differansen mellom lengden og de høyere vektene i motsatt rekkefølge, dvs $d_1(C)$ korresponderer til $n - max\{s|\Delta_s = \Delta_{s+1}\}$ og $d_k(C)$ korresponderer til $n - min\{s|\Delta_s = \Delta_{s+1}\}$. Generelt vil de høyere vektene være gitt ved:

$$d_1(C) = n- \text{ tall nr. } k \text{ i } \{s|\Delta_s = \Delta_{s+1}\}$$

$$d_2(C) = n- \text{ tall nr. } k-1 \text{ i } \{s|\Delta_s = \Delta_{s+1}\}$$

$$\vdots$$

$$d_k(C) = n- \text{ tall nr. } 1 \text{ i } \{s|\Delta_s = \Delta_{s+1}\}$$

Av Bemerkning 3.2.3 ser vi at de duale vektene i det konkrete tilfellet med $[15, 11]$-hammingkoden er gitt ved: $\{8, 12, 14, 15\}$. Generelt vil de høyere vektene til $C^\perp$ følge ved å kombinere dualitetsTeoremet for høyere vekter(se Teorem 3.20) og utrykkene for $d_i(C)$ for $i = 1, .., k$:

$$d_1(C^\perp) = \text{tall nr. } 1 \text{ i } \{s|\Delta_s - 1 = \Delta_{s+1}\}$$

$$d_2(C^\perp) = \text{tall nr. } 2 \text{ i } \{s|\Delta_s - 1 = \Delta_{s+1}\}$$

$$\vdots$$

$$d_k(C^\perp) = \text{tall nr. } n-k \text{ i } \{s|\Delta_s - 1 = \Delta_{s+1}\}$$

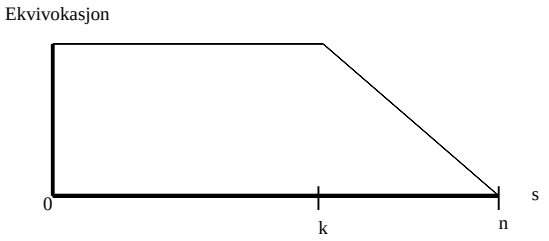
3.3 Ekvivokasjonen til MDS, nær-MDS, nesten-MDS koder og h-MDS-koder

Vi har tidligere beskrevet MDS, nær-MDS og nesten-MDS koder ved de høyere vektene til en kode. Vi ser nå hvordan vi kan beskrive disse kodene ved ekvivokasjonen.

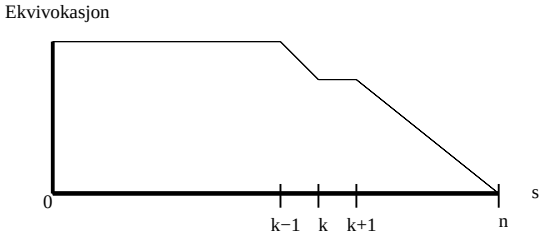
For en MDS-kode er de høyere vektene påfølgende. Vi har at $\Delta_s = \Delta_{s+1}$ for $1 \leq s \leq k-1$ og $\Delta_s = \Delta_{s-1} - 1$ for $k+1 \leq s \leq n$. Grafisk er dette illustrert i figur 3.2:

For en nær-MDS kode vil de høyere vektene være gitt ved: $d_1(C) = d$, $n+1-d_1(C^\perp) = d+1$, $d_2(C) = d+2$, ..., $d_k(C) = k+d$. Vi får da at $\Delta_{s-1} = \Delta_s$ for $1 \leq s \leq k-1$, $\Delta_k = \Delta_{k-1} - 1$, $\Delta_k = \Delta_{k+1}$ og $\Delta_s = \Delta_{s+1} - 1$ for $k+1 \leq s \leq n-1$, som vist i Figur 3.3.

For en nesten-MDS-kode vil de høyere vektene være gitt ved: $d_1(C) = d$, ... , $d_i(C) = d+i-1$, $n+1-d_1(C^\perp) = d+i$, $d_{i+1}(C) = d+i+1$, ... , $d_k(C) = k+d$. Ekvivokasjonskurven er vist i Figur 3.4.

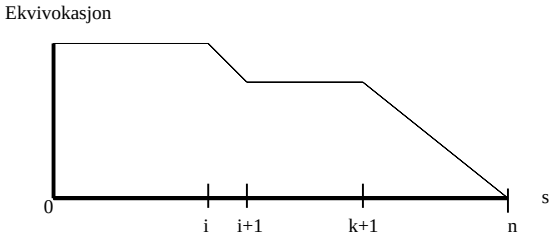


Figur 3.2: Ekvivokasjonskurven til en MDS-kode



Figur 3.3: Ekvivokasjonskurven til en nær-MDS-kode

Vi ser at for en MDS-kode vil ekvivokasjonen forholde seg konstant for $1 \leq s \leq k$. Det betyr at ved å avlytte k informasjonsbiter vil avlytter ikke få noe informasjon. MDS-koder er derfor de mest robuste kodene ved bruk av "wire-tap" kanal.
For en nær-MDS kode vil avlytter ved å få kjennskap til den k-te informasjonsbiten få ekvivokasjonen redusert. Deretter vil den forholde seg konstant til og med den $k+1$-te informasjonsbiten. Nær-MDS koder er derfor de mest robuste kodene etter MDS-koder.
For en nesten-MDS som ikke er nær-MDS-kode vil avlytter ved å få kjennskap til den i-te informasjonsbiten få ekvivokasjonen redusert. Deretter vil den forholde seg konstant til og med den $k+1$-te informasjonsbiten. Nesten-MDS koder er generelt mindre robuste enn nær-MDS koder.
Det kan være naturlig å gi et mål på hvor robust en kode er ved kanalavlytting.



Figur 3.4: Ekvivokasjonskurven til en nesten-MDS-kode

Definisjon 3.3.1. *La $\Delta_s = f(s)$ være ekvivokasjonskurven til en lineær $[n,k]$-kode C. La $f_{opt}(s)$ være ekvivokasjonskurven til en MDS-kode med samme lengde og dimensjon(vi varierer da minimumsdistansen d slik at singletonbegrensningen er oppfylt med likhet). MDS-defekten til C er gitt ved:*

$$def(C) = \sum_{s=0}^{n} (f_{opt}(s) - f(s))$$

MDS-defekten kunne også vært uttrykt ved å summere over differansen mellom de høyere vektene til C og de høyere vektene til en korresponderende MDS-kode(disse er påfølgende). Alternativt kunne $def(C)$ også vært uttrykt ved summen av differansene mellom de duale vektene til C og de korresponderende vektene til en $[n, n-k]$-MDS-kode. Dvs:

$$def(C) = \sum_{i=0}^{k} (d_{i,opt}(C) - d_i(C)) = \sum_{i=0}^{n-k} (d^{\perp}_{i,opt}(C) - d^{\perp}_i(C))$$

MDS-defekten angir hvor mange biter der ekvivokasjonskurven avviker fra ekvivokasjonskurven til koden om den ville vært MDS. Geometrisk kan vi si at $def(C)$ er arealet mellom $f(s)$ og $f_{opt}(s)$. MDS-defekten til en MDS-kode er 0, og for en nær-MDS-kode lik 1.

Eksempel 3.3.2. *Betrakt $[15,11]$-hammingkoden(Se Figur 3). For $0 \leq s \leq 7$ og $13 \leq s \leq 15$ vil $f_{opt}(s) - f(s) = 0$. For $8 \leq s \leq 12$ vil $f_{opt}(s) - f(s) = 1$. MDS-defekten er da gitt ved: $def(C) = 5$*

Vi undersøker nå hvordan ekvivokasjonen henger sammen med singletondefekten og h-MDS.

Vi husker at en kode er h-MDS hvis h er det minste tallet slik at $d_h = n-k+h$. Hvis $h = 1$ vil C være 1-MDS(dvs MDS). Ekvivokasjonskurven forholder seg da konstant til og med k(se Figur 3.2). Hvis C er h-MDS vil ekvivokasjonskurven falle på plass $h-1$ før k. Dvs:

C er h-MDS hvis $h = k - t + 1$, der $t = min\{s|\Delta_s - 1 = \Delta_{s+1}\}$

Vi husker at singletondefekten er gitt ved $S(C) = n - k + 1 - d$. Hvis $S(C) = 0$ er C MDS. Ekvivokasjonskurven vil da forholde seg konstant til og med k for så å være en lineær linje i $n-k$ enhetssteg fra k til n(Se Figur 3.2). Singletondefekten er da lik differansen mellom den minste s i mengden som korresponderer til ekvivokasjonskurven idet den avtar konstant og dimensjonen k. Dvs:

$S(C) = s_0 - k$, der $s_0 = min\{s|\Delta_i - 1 = \Delta_{i+1}, s \leq i \leq n\}$

Eksempel 3.3.3. *Av Figur 3.1 ser vi at $[15,11]$-koden er singletondefekten gitt ved: $S(C) = 13 - 11 = 2$. Tilsvarende ser vi at $h = 11 - 7 + 1 = 5$. Dette er i overenstemmelse med at $S(C) = 15 - 11 + 1 - 3 = 2$ og $d_5 = 15 - 11 + 5 = 9$ mens $d_4 = 7$*

Vi ser at singletondefekten angir hvor mange fall(med et fall mener vi en sammenhengende punktmengde der $\Delta_i = \Delta_{i+1} - 1$ for alle i inneholdt i punktmengden) ekvivokasjonskurven har$(S(C) + 1)$. Den angir også en øvre skranke for hvor mange fall kurven kan ha før k. Vi har at h-MDS angir når avlytter får ekvivokasjonen redusert for første gang.

3.4 "Wire-tap" kanal med matrise i to deler

Vi ser nå på en situasjon hvor vi har to sendere som hver skal sende heholdsvis r_1 og r_2 informasjonsbiter over samme kanal. Også her bruker vi en $\mathbf{x} = [x_1, ..., x_n]$ og er en $(r \times n)$-matrise A, der $A\mathbf{x} = \mathbf{y}$. Vi har at $r = r_1 + r_2$. Vi sender $\mathbf{x} = [x_1, ..., x_n]$. La $Y = (Y^1, Y^2)$ der Y^1 er bitene til første sender og Y^2 er bitene til andre sender. Anta at avlytter har kjennskap til Y^2. Ekvivokasjon til informasjonen inneholdt i Y er gitt ved:

$$\Delta_{1|2:s} = minH(Y^1|Z^\sigma, Y^2),$$

hvor Z^σ er begivenheten at du kjenner x_i, for $i \in \sigma$, der $\sigma \subseteq \{1, ..., n\}$ med kardinalitet s

Matrisen A kan deles inn i to deler: $A = (A^1, A^2)^T$, der A^1 er $r_1 \times n$ matrise og A^2 er $r_2 \times n$ matrise. Følgende resultat generaliserer Proposisjon 3.1.4.

Teorem 3.4.1. *La A, A^1 og A^2 være som beskrevet ovenfor. Da vil:*

$$\triangle_{1|2:s} = min_{\sigma:|\sigma|=n-s}[rang[(A^1_{l_1}, ..., A^1_{l_{n-s}}), (A^2_{l_1}, ..., A^2_{l_{n-s}})]^T - rang(A^2_{l_1}, ..., A^2_{l_{n-s}})]$$

der $\sigma = \{l_1, ..., l_{n-s}\} \subseteq \{1, ..., n\}$

Bevis. Se [LMVC] □

Kapittel 4

Dimensjon/Lengde profil

4.1 Projeksjoner, underkoder og DLP

[F] gir en beskrivelse av lengde/dimensjon profil (LDP) og dimensjon/lengde profil (DLP) for lineære koder C. Vi skal se at LDP til en kode C er det samme som de høyere vektene til C. Før vi beskriver LDP og DLP definerer vi forkorting og punktering av en kode C.

Definisjon 4.1.1. *La C være en $[n,k]$-kode C og la $J \subseteq \{0,1,...,n\} = I$. Den forkortede koden, C_J(også kalt underkode), er definert ved:*

$$C_J\{(c_1,...,c_n) \in C : c_t = 0, t \notin J\}$$

Definisjon 4.1.2. *La J og C være definert som ovenfor. Den punkterte koden, $P_J(C)$(også kalt projeksjonen), er definert ved:*

$$P_J(C) = \{P_J(c) : c = (c_1,...,c_n) \in C\},$$

der komponentene til c er gitt ved: c_t hvis $t \in J$, og $c_t = 0$ hvis $t \notin J$

Lengden til C_J og $P_J(C)$ er lik lengden til C. Det er lett å se at vi har følgende begrensning for støttevekten: $\chi(C_J) \leq \chi(P_J(C)) \leq |J|$ og for dimensjonen: $k(C_J) \leq k(P_J(C)) \leq k$.

Vi gjengir følgende resultat fra [F] som viser hvordan dimensjonene til C_J, $P_{I-J}(C)$, $P_J(C^\perp)$ og $(C^\perp)_{I-J}$ er bestemt av hverandre:

Teorem 4.1.3. *La C være en $[n,k]$-kode og la $C^\perp$ være en $[n,n-k]$-kode. La $J \subseteq I$. Da vil:*

$$dimP_{I-J}(C) + dim(C_J) = k, \qquad dimP_J(C^\perp) = |J| - dim(C_J)$$

$$dim(C^\perp)_{I-J} = n - k - |J| + dim(C_J)$$

Bevis. Se [F] □

Eksempel 4.1.4. *Betrakt* $[7,4,3]$*-hammingkoden. Se Eksempel 1.3.29 for en representasjon av en generatormatrise. La* $J = \{3,4\}$*. Da vil* $I - J = \{1,2,5,6,7\}$*. Generatormatrisene til* C_{I-J} *og* $P_J(C)$ *er gitt ved:*

$$\mathbf{G(C_{I-J})} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\mathbf{G(P_J(C))} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Vi har at $dim(C_{I-J}) = 2$ *og* $dim(P_J(C)) = 2$*, som er i overenstemmelse med at* $dim(C_{I-J}) + dim(P_J(C)) = 2 + 2 = 4 = dim(C)$

Vi definerer nå dimensjon/lengde profil(DLP):

Definisjon 4.1.5. *Dimensjon/lengde profil(DLP) til en kode* C *er gitt ved mengden:*

$$k(C) = \{k_i(C), 0 \leq i \leq n\},$$

hvor komponentene $k_i(C)$ *er den maksimale dimensjonen til en underkode med* $|J| = i$*:*

$$k_i(C) = max_J\{k(C_J) : |J| = i\},\ 0 \leq i \leq n$$

Tilsvarende kan vi definere lengde/dimensjon profilen(LDP) til en kode.

Definisjon 4.1.6. *Lengde/dimensjon profil(LDP) til en kode* C *er gitt ved mengden:*

$$m(C) = \{m_j(C), 0 \leq j \leq k\},$$

hvor komponentene $m_j(C)$ *er den minimale støttevekten til en underkode* C_J *med dimensjon* j*:*

$$m_j(C) = min_J\{|J| : dim(C_J) = j\},\ 0 \leq j \leq k$$

Vi gjengir følgende resultat som et korollar til Teorem 3.4.1. Resultatet viser at $m_j(C)$ korresponderer til de høyere vektene:

Korollar 4.1.7. *La* C *være en* $[n,k]$*-kode og* $C^{\perp}$ *en* $[n, n-k]$*-kode. Da vil:*

$$m_j(C) = min_J\{|J| : k - dim[P_{I-J}(C)] = j\}$$

$$= min_J\{|J| : |J| - dim[P_J(C^\perp)] = j\}$$

$$= min_J\{|J| : dim[(C^\perp)_{I-J}] - n + k + |J| = j\}$$

Vi har at $dim[P_J(C^\perp)]$ svarer til rangen til undermatrisen av generatormatrisen til $C^\perp$ (svarer til paritetssjekkmatrisen til H) som består av kolonnene til undermatrisen indeksert ved J. Derfor vil det tredje uttrykket i Korollar 4.1.7 svare til Teorem 1.3.20. Da vil $m_j(C)$ svare til de høyere vektene, $d_j(C)$, og LDP vil svare til vekthierarkiet. Så fra nå av vil $d_j(C)$ og $m_j(C)$ være ensbetydende for lineære koder.

Vi undersøker nå sammenhengen mellom $m_j(C)$ og $k_j(C)$. Vi har at $m_j(C)$ er det minste tallet i slik at $k_i(C) \geq j$ og $k_j(C)$ er største j slik at $m_j(C) \leq i$. Vi har at $k_i(C)$, for $0 \leq i \leq n$ er ikke-avtagende og $k_{i+1}(C) - k_i(C) \leq 1$(Dette følger av at $dim(C_j) = k - k[P_{I-J}(C)] \geq k - |I - J|$). Derfor vil DLP øke fra 0 til k i k enhetssteg. Hvis $k_{i+1}(C) - k_i(C) = 1$ vil $m_j(C) = i + 1$ for $j = k_{i+1}(C)$. Vi illustrerer denne sammenhengen med et Eksempel:

Eksempel 4.1.8. *La C være $[15, 11]$-hammingkoden. Av Eksempel 1.2.29 har vi at vekthierarkiet er gitt ved:*

$$\{0, 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15\}$$

DLP er da gitt ved:

$$\{0, 0, 0, 1, 1, 2, 3, 4, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Vi definerer nå den inverse DLP.

Definisjon 4.1.9. *Den inverse DLP er gitt ved mengden:*

$$\tilde{k}(C) = \{\tilde{k}_i(C), 0 \leq i \leq n\},$$

hvor komponentene $\tilde{k}_i(C)$ er gitt ved:

$$\tilde{k}_i(C) = max_J\{dim(P_J(C)) : |J| = i\},\ 0 \leq i \leq n$$

Neste resultat viser hvordan DLP og invers DLP er bestemt av hverandre:

Teorem 4.1.10. *Sammenhengen mellom DLP og invers DLP for en lineær kode er gitt ved:*

$$k_i(C) + \tilde{k}_{n-i}(C) = k,\ 0 \leq i \leq n$$

Bevis. Se [F] □

Neste resultat viser at også DLP til en lineær kode og den inverse DLP til dualkoden er bestemt av hverandre:

Teorem 4.1.11. *La C være en $[n,k]$-kode og la $C^{\perp}$ være dualkoden. Da vil:*

$$k_i(C) + \tilde{k}_i(C^{\perp}) = i, 0 \leq i \leq n$$

Vi illustrerer disse sammenhengene med et eksempel:

Eksempel 4.1.12. *Av Eksempel 4.1.8 har vi at DLP er gitt ved:*

$$\{0,0,0,1,1,2,3,4,4,5,6,7,8,9,10,11\}$$

Av Teorem 4.1.10 får vi at den inverse DLP til C er gitt ved:

$$\{0,1,2,3,4,5,6,7,7,8,9,10,10,11,11,11\}$$

Av Bemerkning 3.2.3 har vi at DLP til $C^{\perp}$ er gitt ved:

$$\{0,0,0,0,0,0,0,0,1,1,1,2,2,2,3,4\}$$

Av Teorem 4.1.11 har vi at invers DLP til $C^{\perp}$ er gitt ved:

$$\{0,1,2,2,3,3,3,3,4,4,4,4,4,4,4,4\}$$

4.2 DLP til matroider

Vi ser nå på DLP til matroider og senere for grafer. Fra tidligere vet vi at $\{d_h(M)|1 \leq h \leq n-r\}$ er vekthierarkiet til matroiden M(svarer til de høyere vektene til vektormatroiden $M[H]$).

Vi definerer nå DLP og invers DLP for en matroide:

Definisjon 4.2.1. *La M være en matroide med rang r og høyere vekter $d_j(M)$, $1 \leq j \leq n-r$. DLP til M er gitt ved:*

$$k(M) = \{k_i(M)|0 \leq i \leq n\}$$

hvor komponentene $k_i(M)$ er gitt ved:

$$k_i(M) = max\{j|d_j(M) \leq i\}$$

Merk at $d_j(M)$ er den minste i slik at $k_i(M) \geq j$

Definisjon 4.2.2. *La M være en matroide. La M^* være den duale matroiden med rang $n-r$ og med høyere vekter $d_j(M^*)$, $1 \leq j \leq r$. Invers DLP til M er gitt ved:*

$$\tilde{k}(M) = \{\tilde{k}_i(M)|0 \leq i \leq n\}$$

hvor komponentene $\tilde{k}_i(M)$ er gitt ved:

$$\tilde{k}_i(M) = i - k_i(M^*)$$

Vi ser at vi har definert DLP og invers DLP kun ved de høyere vektene til matroiden. For å kunne formulere analogene til resultatene som inneholder forkortede og punkterte koder må vi omforme disse operasjonene til matroidespråk. Vi husker fra Kapittel 1 Definisjonen av sletting og kontraksjon. Vi undersøker nå sammenhengen mellom matroideoperasjonene sletting/kontraksjon og kodeoperasjonene punktering/forkorting. Slettingen av $E-J$ fra M er gitt ved:

$$M \setminus (E-J) = (E-(E-J), I(M \setminus (E-J))) = (J, I(M\ E-J)), \text{ der}$$

$$I(M \setminus (E-J)) = \{X \subseteq E-(E-J)|X \in I(M)\} = \{X \subseteq J|X \in I(M)\}$$

Altså vil $M \setminus (E-J)$ bestå av grunnmengden J og de uavhengige mengdene i J er de mengdene som er inneholdt i J og som er uavhengige mengder til M(dvs inneholdt i $I(M)$). Dette svarer til det som skjer med matroiden til generatormatrisen, $M[G]$, for en lineær kode C, når vi punkterer mengden J fra C. På grunnlag av dette definerer vi følgende:

Definisjon 4.2.3. *La M være en matroide på grunnmengden E. La $J \subseteq E$. Vi definerer den punkterte matroiden, $P_J(M)$, som:*

$$P_J(M) = M \setminus (E-J).$$

Tilsvarende vil kontraksjonen av $(E-J)$ fra M være gitt ved:

$$M/(E-J) = (M^* \setminus (E-J))^*$$

Dette svarer til det som skjer med matroiden $M[G]$ for en generatormatrise G for en lineær kode C, når vi forkorter mengden J fra koden C(Forkorting av koder får vi ved å punktere J fra dualkoden og så dualisere. Da den duale til matroiden til en kode er matroiden til den duale koden blir dette riktig). Av dette definerer vi:

Definisjon 4.2.4. *La M være en matroide på grunnmengden E. La $J \subseteq E$. Vi definerer den forkortede matroiden, M_J, som:*

$$M_J = M/(E - J)$$

Vi gjengir Teorem 4.1.3 i matroidespråk:

Teorem 4.2.5. *La M være en matroide på grunnmengden E. La $J \subseteq E$ og la rangen være lik $r(M)$. Da vil:*

$$\textit{1) } r(P_{E-J}(M)) + r(M_J) = r(M), \qquad \textit{2) } r(P_J(M^*)) = |J| - r(M_J)$$

$$\textit{3) } r(M^*)_{E-J} = r(M^*) - |J| + r(M_J) = |E - J| - r(M) + r(M_J)$$

Bevis. Vi begynner med å vise 1). Vi har at:

$$r(P_{E-J}(M)) + r(M_J) = r(M \setminus J) + r((M^* \setminus (E - J))^*)$$

$$= r_M(E - J) + |J| - r_{M^*}(E \setminus (E - J)) = r_M(E - J) + |J| - r_{M^*}(J)$$

$$= r_M(E - J) + |J| - (|J| + r_M(E - J) - r_M(E)) = r_M(E) = r(M)$$

Den fjerde likheten følger av Proposisjon 1.2.12. Den siste likheten følger av at rangen til matroiden er lik rangen til grunnmengden E. Med uttrykket $r_M(E)$ mener vi rangfunksjonen til M på mengden E. □

Viser så 2) ved:

$$r(M^* \setminus (E - J)) = r_{M^*}(E - (E - J)) = r_{M^*}(J)$$

$$= |J| - (|J| - r_{M^*}(J)) = |J| - r((M^* \setminus (E - J))^*) = |J| - r(M_J)$$

Viser så 3). Ved å bruke 1) for M^* istedenfor M og $|E - J|$ istedenfor J får vi:

$$r(M^*_{E-J}) = |E| - r(M) - r(P_J(M^*)) = r(M^*) - r(P_J(M^*))$$

For å vise at dette er $r(M^*) - |J| + r(M_J)$ må vi vise at:

$$-r(P_J(M^*)) = -|J| + r(M_J)$$

Men dette følger direkte av 2). Da er 3) bevist.

Proposisjon 4.2.6. *La M være en matroide på grunnmengden E og la $J \subseteq E$. La M^* være dualmatroiden. Da vil:*

$$i)\ k_i(M) + \tilde{k}_{n-i}(M) = r(M^*)$$

$$ii)\ k_i(M) = max_J\{r(M_J^*)||J| = i\}$$

$$iii)\ \tilde{k}_i(M) = min_J\{r(P_J(M^*))||J| = i\}$$

Bevis. Vi begynner med å vise i). Av Definisjon 4.2.2 har vi at invers DLP er gitt ved:

$$\tilde{k}_i = i - k_i(M^*)$$

i) kan da uttrykkes ved:

$$k_i(M) + (n - i) - k_{n-i}(M^*) = r(M^*)$$

Dvs:

$$k_i(M) - k_{n-i}(M^*) = r(M^*) - n + i$$

La $i = 0$. Da vil:

$$k_0(M) = 0, \quad k_{n-0}(M^*) = k_n(M^*) = n - r(M^*)$$

som gir:

$$k_0(M) - k_n(M^*) = 0 - (n - r(M^*)) = r(M^*) - n$$

Har at i) holder for $i = 0$. Vi ser nå hva som skjer i spranget $i \hookrightarrow i + 1$. Vi har at:

$$k_{i+1}(M) - k_i(M) = 1, \text{ hvis } i + 1 = d_j(M^*), \text{ for } 1 \leq j \leq r(M^*). \text{ Og 0 ellers.}$$

$$k_{n-i}(M^*) - k_{n-(i+1)}(M^*) = 1, \text{ hvis } n - i = d_l(M), \text{ for } 1 \leq l \leq r(M). \text{ Og 0 ellers.}$$

Dualitetsteoremet for høyere vekter til matroider(Se Proposisjon 2.1.5) sier at j, for $1 \leq j \leq n$ enten er en høyere vekt til M eller $n + 1 - j$ er en høyere vekt til M^*(Disse tilfellene vil gjensidig utelukke hverandre). Av dette får vi.

$$i+1 = d_j(M),\ 1 \leq j \leq r(M) \quad \Longleftrightarrow$$

$$n+1-(i+1) = n-i \neq d_l(M^*),\ 1 \leq l \leq r(M^*)$$

Derfor vil:

$$k_{i+1}(M) - k_i(M) = 1 \quad \Longleftrightarrow$$

$$k_{n-i}(M^*) - k_{n-(i+1)}(M^*) = 0$$

Vi har da at:

$$k_{i+1}(M) - k_i(M) + k_{n-i}(M^*) - k_{n-(i+1)}(M^*) = 1$$

som gir

$$[k_{i+1}(M) - k_{n-(i+1)}(M^*)] - [k_i(M) - k_{n-i}(M^*)] = 1$$

Vi har derfor at venstre side øker med 1 i spranget $i \hookrightarrow i+1$, og likeledes for høyre side. Formel i) holder derfor for alle i, $0 \leq i \leq n$.

Viser ii). Av Definisjon 4.1.1 har vi at:

$$k_i(M) = max\{j | d_j(M) \leq i\}$$

Dette kan omformes til:

$$max\{j | min_J\{|J| | r(M_J^*) = j\} \leq i\}$$

Vi skal nå vise at dette er det samme som:

$$max_J\{r(M_J^*) | |J| = i\}$$

Anta at vi har har en funksjon f:

$$f : P(E) \longrightarrow Z,$$

som tilfredstiller aksiomene i)' og ii)' for rangfunksjonen til en matroide. La:

$$d_j(M) = min\{|J| | f(J) = j\}$$

Da vil:

$$max\{j | d_j(M) \leq i\} = h(i)$$

$$= max_J\{f(J)||J| = i\} = g(i)$$

At $h(i) = g(i)$ kan vi vise ved at $h(i)$ og $g(i)$ øker med 1 i de samme sprangene.
For $i = 0$ vil $h(0) = g(0) = \emptyset$. Vi ser at $h(i) = j$, når $i \in [d_j, d_{j+1} - 1]$. I spranget $i \hookrightarrow i + 1$ vil $h(i)$ forholde seg konstant dersom både $h(i)$ og $h(i + 1)$ ligger mellom det samme paret av høyere vekter. Og $h(i + 1) = h(i) + 1$ dersom $h(i + 1)$ har samme verdi som en høyere vekt.
Viser nå at $g(i) = j$, når $i \in [d_j, d_{j+1} - 1]$. La $i \in [d_j, d_{j+1} - 1]$. Da finnes det en J med $|J| = d_j$ slik at $f(J) = j$. La $J' = J \cup \{e_1, ..., e_{i-d_j}\}$ slik at $|J'| = d_j + (i - d_j) = i$ Da vil $f(J') \geq f(J) = j$, som gir at $g(i) \geq j$. Det gjenstår da å vise at $g(i) \leq j$. Anta det motsatte. Da vil det eksistere J'' med $|J''| = i$ slik at $f(J'') = j'' > j$. Men dette vil gi at $d_{j''} \leq i$, som igjen gir $d_{j''} < d_{j+1}$. Dette betyr at $j'' < j + 1$(Dette følger av monotomiegenskapen for høyere vekter) som er en selvmotsigelse. Vi har derfor at $g(i) = j$, for $i \in [d_j, d_{j+1} - 1]$. På grunnlag av dette ser vi at $g(i)$ forholder seg konstant i spranget $i \hookrightarrow i + 1$ hvis i og $i + 1$ ligger mellom det samme paret av høyere vekter. Hvis $i + 1$ har samme verdi som en høyere vekt vil $g(i + 1) = g(i) + 1$. Vi har da at:

$$g(i + 1) = g(i) \Longleftrightarrow h(i + 1) = h(i),$$

og tilsvarende:

$$g(i + 1) = g(i) + 1 \Longleftrightarrow h(i + 1) = h(i) + 1$$

Da følger beviset for del (ii) ved å bruke $f(i) = max_J\{r(M_J)^*||J| = i\}$. Vi har at $f(i) = max_J\{r(M_J)^*||J| = i\} = max_J\{|J| - r(J)||J| = i\}$, tilfredsstiller aksiomene (i)' og (ii)' for rangfunksjoner fra Kap. 1. Vi merker oss at dette er samme funksjon som $F(J)$ i beviset for Prop. 2.1.5.

Viser til slutt iii). Av Definisjon 4.2.2 har vi at:

$$\tilde{k}_i(M) = i - k_i(M^*)$$

Vi kan da omforme iii) til:

$$k_i(M^*) = i - min_J\{r(P_J(M^*))||J| = i\}$$

Dette vil igjen være ekvivalent med:

$$k_i(M^*) = max_J\{|J| - r(P_J(M^*))||J| = i\}$$

Ved å bruke ligning 2) i Teorem 4.2.5 får vi:

$$k_i(M^*) = max_J\{r(M_J)||J| = i\}$$

Av Definisjon 4.2.1 har vi.

$$k_i(M^*) = max\{j|d_j(M^*) \leq i\}$$

At de siste to beskrivelsene er identiske følger av beviset for del ii), med M^* for M □

Vi definerer nå LDP for matroider.

Definisjon 4.2.7. *La M være en matroide på grunnmengden E og la $J \subseteq E$. LDP til M er definert ved:*

$$m(M) = \{m_j(M)|0 \leq j \leq n\}$$

der komponentene er gitt ved:

$$m_j(M) = min\{i|k_i(M) \geq j\}$$

Som for koder vil LDP svare til vekthierarkiet(Se bemerkningen under Definisjon 4.2.1). Vi tar med matroideversjonen til Korollar 4.1.7

Korollar 4.2.8. *La M være en matroide på grunnmengden E. La $J \subseteq E$ og la M^* være dualmatroiden. Da vil:*

$$m_j(M) = min_J\{|J| : r(M_J^*) = j\}\ 1)$$

$$= min_J\{|J| : r(M^*) - r[P_{E-J}(M^*)] = j\}\ 2)$$

$$= min_J\{|J| : |J| - r[P_J(M)] = j\}\ 3)$$

$$= min_J\{|J| : r[(M)_{E-J}] - r(M) + |J| = j\}\ 4)$$

Bevis. Vi ser at 3) følger av tilsvarende sats for $d_j(M)$. Derfor er det nok å vise at formlene 1), 2), 3) og 4) er de samme. Ved å dualisere M i 1) og 2) vil likhet følge av 1) Teorem 4.2.5.
Betrakt $m_j(M)$ på grunnmengden $E - J$ istedenfor J. Viser nå at 1) og 3) er like. Formel 1) kan uttrykkes ved:

$$min_J\{|E - J||r(M^*)_{E-J} = j\}$$

Ved 4.2.5 del 3) er dette:

$$min_J\{|E - J||r(M_J) - r(M) = j\}$$

Av 1) Teorem 4.2.5 vil:

$$r(M_J) - r(M) = -r(P_{E-J}(M))$$

Dermed omformes uttrykket til:

$$min_J\{|E-J|||E-J|-r(P_{E-J}(M))=j\}$$

Men dette er det samme som:

$$min_J\{|J|||J|-r(P_J(M))=j\},$$

som svarer til 3) Teorem 4.2.5

Tilsvarende vil 4) betraktet på grunnmengden $|E-J|$ være gitt ved:

$$min_J\{|E-J||r(M_J)-r(M)+|E-J|=j\}$$

At dette svarer til likhet 1) følger av Teorem 4.2.5 del 3). □

4.3 Sammenhengen mellom DLP og Ekvivokasjon

Vi definerte DLP til en kode C i Definisjon 4.1.5. Da DLP og LDP er bestemt av hverandre og LDP svarer til vekthierkiet vil DLP og de høyere vektene være bestemt av hverandre. Vi har tidligere sett at de høyere vektene og ekvivokasjonen bestemmer hverandre. Vi ser nå på hvordan vi kan finne ekvivokasjonen ved hjelp av DLP.

Av Eksempel 4.1.8 har vi at DLP til $[15, 11]$-Hammingkoden er gitt ved:

$$\{0,0,0,1,1,2,3,4,4,5,6,7,8,9,10,11\}$$

De høyere vektene er gitt ved:

$$\{0,3,5,6,7,9,10,11,12,13,14,15\}$$

Av Eksempel 4.1.12 er ekvivokasjonen gitt ved:

$$\{4,4,4,4,4,4,4,4,3,3,3,3,2,2,1,0\}$$

Vi ser at ekvivokasjonen forholder seg konstant i det den omvendte følgen til DLP avtar med 1 fra høyre. Ekvivokasjonen avtar med 1 i det den omvendte følgen DLP forholder seg konstant. I vårt tilfelle har vi da at:

$$\triangle_s = (n-s) - \tilde{k}_{n-s}(C),\ 0 \leq s \leq n$$

Av Eksempel 4.1.12 er Invers DLP gitt ved:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 7, 8, 9, 10, 10, 11, 11, 11\}$$

Ekvivokasjonen forholder seg konstant i det Invers DLP øker. Ekvivokasjonen avtar med 1 i det Invers DLP forholder seg konstant. I dette tilfelle ser vi at:

$$\triangle_s = (n-k) + k_s(C) - s, 0 \leq s \leq n$$

Alternativt kunne formelen vært innsett direkte ved å bruke at: $k_s(C) + \tilde{k}_{n-s}(C) = dim(C)$

Av Eksempel 4.1.12 har vi at Invers DLP til $C^{\perp}$ er gitt ved:

$$\{0, 1, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 4, 4, 4\}$$

Vi ser at dette er den omvendte ekvivokasjonen til $[15, 11]$-Hammingkoden. Dvs:

$$\triangle_s = \tilde{k}_{n-s}(C^{\perp}),\ 0 \leq s \leq n$$

Disse uttrykkene for $\triangle_s$ lar seg lett generalisere. Vi overlater det til leseren å vise at disse uttrykkene holder for koder generelt.

4.4 DLP og ekvivokasjon til en graf

Vi har tidligere definert de høyere vektene til en graf. Da DLP er definert ved hjelp av de høyere vektene kan vi definere DLP til en graf.

De høyere vektene $d_h(G)$ til en graf G angir den minste undergrafen som inneholder h sykler. Da vil 0-ene i DLP vil da svare til antall kanter som utgjør den minste sykelen i grafen. Videre vil 1-erne svarer til den minste undergrafen som inneholder 2 sykler, osv. Da k_i er definert for $0 \leq i \leq n$, vil antall komponenter i DLP være 1 større enn antall kanter til G. Det siste elementet i DLP har derfor ingen grafteoretisk fortolkning.

Eksempel 4.4.1. *Betrakt grafen K_4(se Figur 2.1). Vekthierarkiet(LDP) er gitt ved:* $\{0, 3, 5, 6\}$ *DLP er da gitt ved:*

$$\{0, 0, 0, 1, 1, 2, 3\}$$

Vi fortolker nå ekvivokasjonen for en graf. Vi vet at ekvivokasjonen til en kode svarer til den omvendte inverse DLP til dualkoden. Fra grafteorien følger det av konstruksjonen av den duale til en graf G at en kantmengde er en sykel i G hvis og bare hvis den er en minimal separerende kantmengde(dvs den minste undergrafen som ved å fjerne den fra grafen gjør at antall komponeneter øker med 1) i $G^{\perp}$. Ekvivokasjonen til en graf vil forholde seg konstant dersom vi ved å fjerne en kant ikke kan danne en minimal separerende kantmengde, og avtar dersom vi ved å fjerne en kant kan danne en minimal separerende kantmengde. På grunnlag av dette formulerer vi følgende resultat:

Proposisjon 4.4.2. *Gitt en sammenhengende graf G. Ekvivokasjonsfunksjonen $\triangle_s$ er slik at $\triangle_s = m$, hvis det maksimale antall sammenhengende komponenter vi kan danne ved å fjerne s kanter er $m+1$.*

Eksempel 4.4.3. *Betrakt igjen K_4. Vi har at K_4 er selvdual, så DLP til $K_4^{\perp}$ er lik DLP til K_4. Invers DLP er da gitt ved:*

$$\{0, 1, 2, 2, 3, 3, 3\}$$

Ekvivokasjonen vil da være gitt ved den omvendte følgen. Vi har derfor at $\triangle_0 = \triangle_1 = \triangle_2 = 3$, $\triangle_3 = \triangle_4 = 2$, $\triangle_5 = 1$ og $\triangle_6 = 0$. Vi ser at vi ved å fjerne den tredje kanten får ekvivokasjonen redusert for første gang(Dette svarer til antall kanter i en minimal separerende kantmengde til K_4). Ved å fjerne ytterligere to kanter vil ekvivokasjonen avta igjen.(Dette svarer til antall kanter i en minimal separerende kantmengde til undergrafen vi fikk ved å fjerne den første minimale separerende kantmengden fra K_4). Videre vil ekvivokasjonen avta fra 1 til 0, da vi fjerner den siste kanten i K_4.

Kapittel 5

Relativ dimensjon/lengde profil, relativ rangfunksjon og kvasimatroider

5.1 Relativ dimensjon/lengde profil

Vi har tidligere definert DLP, invers DLP og LDP for en lineær kode C. Vi utvider nå disse konseptene til å gjelde for to-kode format. Dette har sammenheng med ekvivokasjonen til en kode med matrise i to deler som beskrevet i Kapittel 3.4. Vi begynner med å definere analogene til DLP og invers DLP for to-kode format.

Definisjon 5.1.1. *La C^1 være en $[n, k_1]$-kode og la C^2 være en $[n, k_2]$-underkode til C^1. Den relative dimensjon/lengde profilen, RDLP, er definert ved:*

$$K(C^1, C^2) = \{K_i(C^1, C^2) | 0 \leq i \leq n\}, \text{ der}$$

$$K_i(C^1, C^2) = max\{dimC^1_J - dimC^2_J || J| = i\}$$

Definisjon 5.1.2. *La C^1 og C^2 være som beskrvet ovenfor. Den inverse relative dimensjon/lengde profilen, IRDLP, er definert ved:*

$$\tilde{K}(C^1, C^2) = \{\tilde{K}_i(C^1, C^2) | 0 \leq i \leq n\}, \text{ der}$$

$$\tilde{K}_i(C^1, C^2) = min\{dimP_J(C^1) - dimP_J C(^2) || J| = i\}$$

Bemerkning 5.1.3. *Setter vi $k_2 = 0$ har vi de vanlige profilene.*

Vi gjengir følgende resultat som viser at RDLP og IRDLP er bestemt av hverandre.

Teorem 5.1.4. *La C^1 og C^2 være som beskrvet ovenfor. RDLP og IRDLP er relatert ved:*

$$K_i(C^1, C^2) = (k_1 - k_2) - \tilde{K}_{n-i}(C^1, C^2)$$

Bevis. Se [LMVC] □

Vi minner om situasjonen beskrevet i Kapittel 3.4. La A være paritetssjekkmatrisen til koden C^1. Fra Kapittel 3.4 har vi at $A = (A^1, A^2)^T$ var en $r \times n$ matrise i to deler der A^1 var en $r_1 \times n$ matrise og A^2 var en $r_2 \times n$ matrise. A hadde som funksjon å skjule informasjon i $\mathbf{y}$. Vi krypterte $\mathbf{y}$ ved $A\mathbf{x} = \mathbf{y}$ for så å sende $\mathbf{x}$. Kombinerer vi Teorem 3.4.1 og Definisjon 4.5.2 har vi følgende resultat som viser sammenhengen mellom IRDLP og ekvivokasjonen til en kode med matrise i to deler:

Korollar 5.1.5. *La C^1 og C^2 være som før. For $0 \leq s \leq n$ vil:*

$$\triangle_{1|2;s} = \tilde{K}_{n-s}(C^1, C^2)$$

Vi ser at $K(C^1, C^2)$ er et mål for usikkerheten. Som for en kode med enkelt format vil $K(C^1, C^2)$ være ikke-avtagende. Følgende Proposisjon viser at RDLP og IRDLP på det meste kan øke med 1 i spranget $i \hookrightarrow i + 1$.

Proposisjon 5.1.6. *La C^1 og C^2 være som før. For $0 \leq i \leq n - 1$ vil:*

$$0 \leq K_{i+1}(C^1, C^2) - K_i(C^1, C^2) \leq 1$$

$$0 \leq \tilde{K}_{i+1}(C^1, C^2) - \tilde{K}_i(C^1, C^2) \leq 1$$

Vi har også at:

$$K_0(C^1, C^2) = \tilde{K}_0(C^1, C^2) = 0, \text{ og}$$

$$K_n(C^1, C^2) = \tilde{K}_n(C^1, C^2) = k_1 - k_2$$

Bevis. Se [LMVC] □

Tilsvarende definerer vi den relative lengde/dimensjon profilen som en generalisering av LDP som vi tidligere har definert.

Definisjon 5.1.7. *La C^1 og C^2 være som før. Den relative lengde/dimensjon profilen, RLDP, er definert ved:*

$$M(C^1, C^2) = \{M_j(C^1, C^2) | 0 \leq j \leq k_1 - k_2\},\ der$$

$$M_j(C^1, C^2) = min\{dimC_J^1 - dimC_J^2 \geq j\}$$

Vi husker at LDP svarte til de høyere vektene til en kode C. Tilsvarende kan vi si at RLDP svarer til de relative høyere vektene til C. Neste resultat viser relasjonen mellom RDLP og RLDP:

Teorem 5.1.8. *La C^1 og C^2 være som før. Da vil:*

$$M_j(C^1, C^2) = min\{i | K_i(C^1, C^2) \geq j\},\ og$$

$$K_i(C^1, C^2) = max\{j | M_j(C^1, C^2) \leq i\},\ der$$

$0 \leq j \leq k_1 - k_2$ *og* $0 \leq i \leq n$

Bevis. Se [LMVC] □

Kombinerer vi Teorem 5.1.4 og Teorem 5.1.8 ser vi at RDLP, IRDLP og RLDP er bestemt av hverandre.

Vi vet at RDLP er en ikke-avtagende følge fra 0 til $k_1 - k_2$. Fra Teorem 5.1.8 har vi da at: $M_j(C^1, C^2) = min\{i | K_i(C^1, C^2) \geq j\} = min\{i | K_i(C^1, C^2) = j\}$, der $0 \leq j \leq k_1 - k_2$. Den siste likheten følger av at: $\{i | K_i(C^1, C^2) = j\} \cap \{i | K_i(C^1, C^2) \geq j+1\} = \emptyset$. Vi ser at RLDP er strengt økende(dette i samsvar med LDP som svarer til de høyere vektene). På grunnlag av dette formulerer vi følgende Proposisjon:

Proposisjon 5.1.9. *La C^1 og C^2 være som før. Da vil:*

$$M_j(C^1, C^2) = min\{i | K_i(C^1, C^2) \geq j\}$$

$$= min\{|J| | dimC_J^1 - dimC_J^2 = j\},\ hvor$$

$M_0(C^1, C^2) = 0,\ og\ 0 \leq j \leq k_1 - k_2$

Vi ser nå på en øvre begrensning, $UP(\tilde{K})$, av $\tilde{K}_s$. Fra Korollar 5.1.5 vet vi at $\tilde{K}_{n-s}$ er ekvivokasjonen til en kode. Vi kan da si at $UP(\tilde{K})$ angir en øvre begrensning for den reverserte ekvivokasjonen. Vi husker at ekvivokasjonen er et mål for usikkerheten, så et par av koder som oppfyller denne begrensningen med likhet vil være de mest robuste ved kanalavlytting(Vi skal senere se at de parene av koder med denne egenskapen er en generalisering av MDS-koder). Vi innfører også to andre begrensninger, $LO(K)$ og $UP(M)$(som er en generalisering av singletonbegrensningen). Først definerer øvre og nedre begrensning av to følger med heltall. O

Definisjon 5.1.10. *Gitt to heltallsfølger* $\{\pi_1, ..., \pi_n\}$ *og* $\{\delta_1, ..., \delta_n\}$. *Vi sier at* $\{\pi_1, ..., \pi_n\}$ *er øvre begrenset av* $\{\delta_1, ..., \delta_n\}$ *hvis* $\pi_i \leq \delta_i$ *for* $0 \leq i \leq n$. *Tilsvarende vil* $\{\pi_1, ..., \pi_n\}$ *være nedre begrenset av* $\{\delta_1, ..., \delta_n\}$ *hvis* $\pi_i \geq \delta_i$ *for* $0 \leq i \leq n$

Neste resultat angir begrensningene $UP(\tilde{K})$, $LO(K)$ og $UP(M)$ for et to-kode format.

Teorem 5.1.11. *La* C^1 *og* C^2 *være som før. Invers RDLP,* $\tilde{K}(C^1, C^2)$ *er øvre begrenset av* $UP(\tilde{K})$ *gitt ved:*

$$\{UP(\tilde{K})_i | 0 \leq i \leq n\} = \{0, ..., 0, 1, 2, ..., k_1 - k_2, ..., k_1 - k_2\},$$

der $max\{i | UP(\tilde{K})_i = 0\} = k_2$.

RDLP, $K(C^1, C^2)$ *er nedre begrenset av* $LO(K)$ *gitt ved:*

$$\{LO(K)_i | 0 \leq i \leq n\} = \{0, ..., 0, 1, 2, ..., k_1 - k_2, ..., k_1 - k_2\},$$

der $max\{i | LO(K)_i = n - k_1\}$.

RLDP, $M(C^1, C^2)$, *er øvre begrenset av* $UP(M)$ *gitt ved:*

$$\{UP(M)_j | 0 \leq j \leq k_1 - k_2\} = \{0, n - k_1 + 1, n - k_1 + 2, ..., n - k_2\}$$

Bevis. Se [LMVC] □

Bemerkning 5.1.12. *Vi ser at* $UP(M)$ *er en generalisering av singletonbegrensningen (RLDP svarer til de relative høyere vektene og da vil* $d_1 \leq n - k_1 + 1$*)*

Neste resultat belyser sammenhengen mellom $UP(\tilde{K})$, $LO(K)$ og $UP(M)$.

Proposisjon 5.1.13. *Dersom en av begrensningene,* $UP(\tilde{K})$, $LO(K)$ *og* $UP(M)$, *er oppfylt med likhet vil alle tre være oppfylt med likhet. Vi har at* $UP(\tilde{K})$ *er oppfylt med likhet hvis og bare hvis* $\tilde{K}_{k_1}(C^1, C^2) = k_1 - k_2$, $LO(K)$ *er oppfylt med likhet hvis og bare hvis* $K_{n-k_1}(C^1, C^2) = 0$ *og* $UP(M)$ *er oppfylt med likhet hvis og bare hvis* $M_1(C^1, C^2) = n - k_1 + 1$

Bevis. Se [LMVC] □

Dersom $k_2 = 0$(som gir at $C^2 = \emptyset$) har vi $M_1(C^1, C^2)$ svarer til den tradisjonelle singletonbegrensningen. Vi har da at C^1 er MDS hvis og bare hvis $M_1(C^1, \emptyset) = n - k_1 + 1$(dvs om den oppfyller singletonbegrensningen med likhet) eller $K_{n-k_1}(C^1, \emptyset) = max\{dimC^1_J || J| = n - k_1\} = 0$, der $J \subseteq \{1, ..., n\}$. Dersom C^1 er MDS har vi da at for en vilkårlig underkode $C^2 \subseteq C^1$ vil: $K_{n-k_1}(C^1, C^2) = max\{dimC^1_J - dimC^2_J || J| = n - k_1\}$. Dette kommer av at vi får 0 for $max\{dimC^1_J || J| = n - k_1 + 1\}$ da vi ikke har noen koderod av vekt $n - k_1$ for MDS-koden C^1. Da vil også fradragsleddet bli 0, som gir at $K_{n-k_1}(C^1, C^2) = 0$. Så dersom C^1 er MDS vil (C^1, C^2) oppfylle $UP(\tilde{K})$, $LO(K)$ og $UP(M)$ med likhet.

Vi undersøker nå om det finnes koder som ikke er MDS, men som oppfyller begrensningene i Proposisjon 5.1.13. La C^1 være en $[n,k,d]$-kode som er nær MDS. Vi har da at:

$$K_{n-k_1}(C^1) = max\{dimC^1_J||J| = n-k_1\} = 1,$$

da det eksisterer kodeord av vekt $n-k_1$, men det ikke eksisterer 2-dimensjonale underrom med støttevekt høyst lik $n-k_1+1$. La C^2 være en underkode av C^1. Dersom C^2 inneholder kodeord av vekt $n-k_1$ vil $K_{n-k_1}(C^2) = 1$. Og videre har vi at hvis C^2 inneholder alle kodeord av vekt $n-k_1$ i C^1 vil $K_{n-k_1}(C^1, C^2) = 0$. Dersom C^2 ikke inneholder et kodeord av vekt $n-k_1$ vil $K_{n-k_1}(C^2) = 0$, som gir $K_{n-k_1}(C^1, C^2) = 1$. Vi får også at $M_1(C^1, C^2) = 1$(dette er en direkte konsekvens av at C er nær-MDS)

Vi har tidligere definert ekvivokasjonen til en kanal med matrise i to deler. Denne er gitt ved:

$$\Delta_{1|2:s} = minH(Y^1|Z^\sigma, Y^2),$$

Av Korollar 5.1.5 har vi at:

$$\Delta_{1|2:s} \leq \tilde{K}_{n-s}(C^1, C^2) = k_1 - k_2$$

Vi har at $k_1 - k_2$ er den maksimale verdien i $UP(\tilde{K})$). Vi observerer at dersom $s \leq k_1$ vil $k_1 - k_2$ bare være en mulig verdi for $\Delta_{1|2:s}$(dette følger av at $UP(\tilde{K}_s)$ bare kan ha denne verdien for $s \geq n-k+1$). Antall 0-er i $UP(\tilde{K})$ vil være lik k_2, deretter vil den øke(ikke nødvendigvis monotont) i $k_1 - k_2$ steg til maksimalverdien $k_1 - k_2$. Dersom vi har $s = n-k+1$(likhet i singletonbegrensningen) får vi at $\Delta_{1|2:s} = k_1 - k_2$ som gir maksimal ekvivokasjon. ($UP(\tilde{K})$ vil da øke monotont fra k_2 til $k_1 - k_2$). For $k_2 = 0$ vil dette svare til $\Delta_{1|2:s} = k$ for den vanlige profilen.
Vi innfører nå et nytt begrep hentet fra kryptografien: "Perfect secrecy". La:

$$H(Y^1|Z^\sigma, Y^2) = H(S^1)\ 1)$$

betegne "perfect secrecy" med hensyn på $\Delta_{1|2:s}$. La $s = 0$ og $A^2 = 0$ i Teorem 3.4.1. Dersom vi ser på den øverste delen av matrisen A^1 med rang $k_1 - k_2$(dvs vi eksluderer de k_2 nederste radene) vil 1) svare til:

$$\tilde{K}(C^1, C^2) = k_1 - k_2(\text{fordi } H(S^1) = k_1 - k_2)$$

Dette svarer til maksimal ekvivokasjon. Dvs. tredjeparten kjenner alle y_i-ene men ingen av x_i-ene. Det at x_i-verdiene blir holdt skjult for avlytter(dvs all informasjon som kan holdes hemmelig for en tredjepart holdes hemmelig) er det som ligger i begrepet "perfect secrecy".

Hvis C^1 og C^2 er "gode" koder vil denne tilstanden av maksimal ekvivokasjon vedvare lengst mulig(dvs i hele området $s \in [o, ..., k_1]$). Dette er ekvivalent med at begrensningene $UP(\tilde{K})$, $LO(K)$ og $UP(M)$ er oppfylt med likhet. I praksis vil dette bety at ved å avlytte k_1 av x_i-ene, i tillegg til de k_2 y_i-ene vil avlytteren ikke få noe mer informasjon enn om han/hun bare hadde avlyttet y_i-ene.

5.2 Relativ rangfunksjon og kvasimatroider

Vi undersøker nå om det lar seg gjøre å formulere teorien i forrige seksjon i matroidespråk. Den relative rangfunksjonen, $R(J)$, vil være gitt ved:

$$R(J) = dimP_J(C^1) - dimP_J(C^2),$$

hvor C^1 er koden med generatormatrise A(av dimensjon k^1) og C^2 er underkoden som består av de k^2 nederste radene i A. Vi undersøker nå om $R(J)$ oppfyller rangaksiomene gitt ved:

i) $0 \leq r(I) \leq |I|$, for alle $I \subseteq E$

ii)Hvis $I \subseteq J \subseteq E$, så er $r(I) \leq r(J)$

iii) Hvis $I, J \subseteq E$, så er $r(I \cup J) + r(I \cap J) \leq r(I) + r(J)$

Eksempel 5.2.1. *La C^1 være en linær kode over F_3 med generatormatrise gitt ved:*

$$\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

La C^2 være underkoden med generatormatrise $\boldsymbol{A}^2 = (1\ 1)$. La $I = \{1\}$ og $J = \{2\}$. Da vil $I \cap J = \emptyset$ og $I \cup J = \{1, 2\}$. Vi har at $R(I \cap J) = 0$, $R(I \cup J) = 1$ og $R(I) = R(J) = 0$. Vi ser at tredje aksiom ikke holder, da venstre side er 1 mens høyre side er 0.

Av Eksempelet ser vi at vi ikke har noen rangfunksjon i det relative tilfellet, og vi har følgelig ingen matroidestruktur. Vi kan også se at vi ikke har noen rangfunksjon ved å bruke at en delmengde, T, er uavhengig dersom $|T| = R(T)$. Videre vil rangen, $R(S)$, være den maksimale kardinaliteten til en uavhengig mengde gitt at vi har en matroide med rangfunksjon R. Av Eksempelet ovenfor har vi at $R(\{\emptyset\}) = R(\{1\}) = R(\{2\})$, mens $R(\{1, 2\})$. Største delmengde av mengden $\{1, 2\}$ som oppfyller at $|T| = R(T)$ er $\emptyset$, men vi har sett at $R(\{S\}) = 1$.

Vi har sett at $R(S)$ ikke oppfyller aksiom 3). Vi viser nå at den oppfyller aksiom 1) og 2) og hvordan vi kan definere en kvasimatroide som ligger nærmest mulig definisjonen til en matroide.

Det er lett å se at aksiom 1) holder. Gitt en delmengde T kan ikke rangen være større enn kardinaliteten. Ser på aksiom 2): Vi har at $R(J) = dimP_J(C^1) - dimP_J(C^2)$, der J er en indeksmengde for kolonner til A. Fjern så kolonnene i A som ligger over indeksene i J, og vi får en matrise A_J. Vi transpornerer så denne matrisen og betegner den $(A_J)^T$. Radene i A som dannet A^2 er nå en delmengde av kolonnerommet til $(A_J)^T$. Det er k_1 rader i A og derfor også k_1 kolonner $(A_J)^T$. For de k_2 kolonnene som utgjør A^2 vil disse svare til en indeksmengde S av kardinalitet k_2 som er inneholdt i indeksmengden $E = \{1, 2, ..., k_1\}$ for kolonnene i $(A_J)^T$. Derfor vil $dimP_J(C_2)$ svare til $dimP_S(D)$, der D er koden som har $(A_J)^T$ som generatormatrise. Videre vil $dimP_J(C_1)$ svare til $dimD$. Vi har da at:

$$R(J) = dimP_J(C^1) - dimP_J(C^2) = dimP_S(D) - dimD$$

Av Teorem 4.1.3 ser vi at det siste uttrykket er ekvivalent med $dimD_{E-S}$. Vi har da at $R(J)$ svarer til dimensjonen til vektorrommet som består av vektorene(kodeordene) i radrommet D til $(A_J)^T$ som er null i S(og derfor ikke null i $E - S$).
La nå $I \subseteq J$. Ved å følge prosedyren ovenfor vil $R(I)$ være lik dimenjonen til vektorrommet som består av vektorene(kodeordene) i D til $(A_J)^T$ som er null i S. Men da I er en delmengde av J vil de radene i $(A_J)^T$ som svarer til indeksene i $J - I$(disse er kolonneindekser til den opprinnelige matrisen A) bli eksludert. Vi ser at de vektorene som oppfyller dette i radrommet D til $(A_J)^T$ også vil gjøre det i det mindre radrommet. Derfor vil $R(I) \subseteq R(J)$.

Vi minner om de alternative rangaksiomene (i)', (ii)", (iii)' fra Teorem 1.2.7:

i)' $r(\emptyset) = 0$

ii)' $r(J) \leq r(J \cup \{x\}) \leq r(J) + 1$

iii)' Hvis $r(J \cup \{x\}) = r(J \cup \{y\}) = r(J)$, så vil $r(J \cup \{x\} \cup \{y\}) = r(J)$

Da aksiom (i) impliserer (i)', og aksiom (i) holder for funksjonen $J \longrightarrow R(J)$, holder aksiom (i)'. Videre vil en minimal revisjon av de siste 5 linjene i beviset for at aksiom (ii) holder for funksjonen R, gi at aksion (ii)' holder. Vi har da at aksiom (i)' og (ii)' holder for R, men ikke (iii)' (for hadde (i)',(ii)',(iii)' holdt, ville det ekvivalente aksiomsettet (i),(ii), (iii) holdt, og (iii) holder ikke, så vi i Eksempel 5.2.1.). Vi vil nå gi et eget navn til slike funksjoner som tilfredsstiller (i)' og (ii)':

Definisjon 5.2.2. *La $E = \{1, 2, ..., n\}$. La $R : P(\{1, 2, ..., n\}) \longrightarrow N \cup \{0\}$ være en funksjon som oppfyller rangaksiom i)' og ii)', men ikke nødvendigvis rangaksiom iii)'. Vi kaller paret (E, R) for en kvasimatroide.*

Definisjon 5.2.3. *La E og R være som ovenfor. La $J \subseteq E$. Vi kaller paret (E, R^*) den duale kvasimatroiden der rangfunksjonen $R^*(J)$ er gitt ved:*

$$R^*(J) = |J| + R(E - J) - R(E)$$

Vi kan se at $R^*(J)$ er den duale rangfunksjonen ved å vise at $(R^*)^*(J) = R(J)$. Vi har at:

$$(R^*)^*(J) = |J| + R^*(E - J) - R^*(E) =$$

$$|J| + (|E - J| + R(J) - R(E)) - (|E| + R(E - E) - R(E)) = R(J)$$

Vi definerer så de høyere vektene, komponentene til DLP, komponentene til invers DLP og dualene til disse.:

Definisjon 5.2.4. *Gitt en kvasimatroide med grunnmengde E med rangfunksjon $R(J)$ og dual rangfunksjon $R^*(J)$. De høyere vektene, d_i, er gitt ved:*

$$d_i = min\{|J||R(J) = |J| - i\}$$

De høyere vektene, d_i^*, er gitt ved:

$$d_i^* = min\{|J||R^*(J) = |J| - i\}$$

Definisjon 5.2.5. *Komponentene til DLP, k_i, er gitt ved:*

$$k_i = max\{j|d_j \leq i\}$$

Komponentene til DLP til den duale kvasimatroiden, k_i^*, er gitt ved:

$$k_i^* = max\{j|d_j^* \leq i\}$$

Definisjon 5.2.6. *Komponentene til invers DLP, $\tilde{k}_i$, er gitt ved:*

$$\tilde{k}_i = i - k_i^*$$

Komponentene til invers DLP til den duale kvasimatroiden, $\tilde{k}_i^*$, er gitt ved:

$$\tilde{k}_i^* = i - k_i$$

Vi vil nå vise analogien til Proposisjon 4.2.6 for kvasimatroider. Den første av de tre påstandene derfra formulerer vi nå slik:

$$k_i + \tilde{k}_{n-i} = R * (E)$$

Dette kan omformuleres til:

$$k_i - k_{n-i}^* = R^*(E) - n + i \ 1)$$

Vi vil først vise 1) for $n = 0$, det vil si: $k_0 = 0$ og $k_n^* = n - R^*(E)$

Da $d_i \geq 1$, for alle $i \geq 1$ har vi at:

$$k_0 = max\{j|d_j \leq 0\} = 0$$

Videre har vi at

$$k_i^* = max\{j|d_j^* \leq n\} = n - R^*(E)$$

Her har vi brukt at hvis $A \subseteq B$ vil $F^*(A) \leq F^*(B)$, eller $F(A) \leq F(B)$. Dette følger av at $|A| - R(A) \leq |B| - R(B) \Longrightarrow R(B) - R(A) \leq |B| - |A|$. Vi har da at $B = A \cup \{x_1, ..., x_s\}$, der $s = |B| - |A|$. Det at 1) holder for i medfører at den holder for $i + 1$, viser vi på samme måte som i tilsvarende sats for matroider i Kapittel 4. En viktig ingrediens er i begge tilfeller aksiom (ii)' fra Teorem 1.2.7.
Den andre påstanden i Proposisjon 4.2.6 omformulerer vi til:

$$k_i = max_J\{|J| - R(J)||J| = i\}$$

Vi har at $k_i = max\{j|d_j \leq i\}$. Men dette følger direkte av beviset for matroider.

Den tredje påstanden i Proposisjon 4.2.6 omformulerer vi til:

$$\tilde{k}_i = min_J(R*(J)||J| = i$$

$$k_i^* = min_J\{R^*(J)||J| = i\}$$

Vi ønsker å omforme dette til en ekvivalent påstand som vi vet er sann. Vi har at:

$$\tilde{k}_i = i - k_i^*$$

Dette kan omformes til:

$$k_i^* = i - min_J\{R^*(J)||J| = i\}$$

som igjen er ekvivalent med:

$$max_J\{|J| - R^*(J)||J| = i\}$$

men dette er det samme som:

$$max_J\{j|d_j^* \leq i\}$$

Dermed holder alle påstandene fra Proposisjon 4.2.6 også i kvasimatroidesammenheng. Videre kan vi vise analogien til dualitetsresultatet, Proposisjon 2.1.5, også for kvasimatroider, da beviset for denne satsen essensielt bare bruker aksiom (i)' og (ii)'.

Kapittel 6

Trelliser og trellisdekoding

6.1 Trelliser

Vi definerer nå en type vektede digrafer kalt trelliser. Vi ser på hvordan disse trellisene kan brukes til dekoding og sammenhengen mellom trelliser og DLP til koden.

La F være et alfabet. En trellis er en digraf der hjørnene er i kolonner $V_0, V_1, ..., V_n$ der V_i er mengden av tilstander(hjørner) i kolonne i. V_0 består av et enkelthjørne som kalles kilden, s, til trellisen. Kantmengden til trellisen er i kolonner $E_{i-1,i}$ for $i = 1, .., n$ der $E_{i-1,i}$ har starthjørne i V_{i-1} og endehjørne i V_i. Hver av kantene er vektet og hver vekt er et element i F. Alle stier fra s til t er av lengde n. En sti kan derfor betraktes som et kodeord til en kode av lengde n, der vektene danner kodeordet. Mengden, C, av alle kodeord representert av en sti i trellisen utgjør koden representert av trellisen. Gitt en villkårlig kode vil denne alltid være representert som en trellis, da vi kan la de $|C|$ kodeordene utgjøre hver sine kant-disjunkte stier der vektene i hver sti danner et kodeord. To trelliser T og $T^{`}$ er isomorfe hvis det eksisterer en en-til-en korrespondanse $f$ fra $V$ til $V^{`}$ slik at $f(V_i) = V_i^{`}$ og gitt at $\alpha$ er en vekt til en kant i $T$ fra $v$ til $v^{`}$ hvis og bare hvis α er en vekt til en kant i $T^{`}$ fra $f(v)$ til $f(v^{`})$.
Gitt en linær $[n, k]$ kode C over F_q kan vi konstruere to forskjellige trelliser som representerer C. Trellisen $\hat{T}(C)$ er et tre der $\hat{V}_i$, mengden av alle tilstander i kolonne i, er mengden av alle forkortinger av lengde i av kodeordene i C. Dvs. Hvis $(a_1, ..., a_n) = c \in C$, la $c_i = (a_1, ..., a_i)$ og la $\hat{V}_i = \{c_i | c \in C\}$. Da vil $\hat{V}_0$ ha et element $\mathbf{0}$ som representerer nullkodeordet. De $i+1$-te kantene til $\hat{T}(C)$ er på formen: $(a_1, ..., a_i) \longrightarrow (a_1, ..., a_{i+1})$. En sti av lengde n må ende i $\hat{V}_n$ som er lik C. Hvis $c = c_n$ er et slutthjørne er det kun kanten c_{n-1} som ender i C. Da vil a_n være den siste koordinaten i kodeordet. Tilsvarende vil kun en kant ende i c_{n-1}. Av induksjon følger det at det eksisterer en unik sti fra $\mathbf{0}$ til c og denne stien utgjør kodeordet c.
Vi sier at T er en ekte trellis hvis V_0 består av et starthjørnet $\mathbf{0}$, alle hjørnene i T er inneholdt i en sti av lengde n og ingen stier av lengde i fra $\mathbf{0}$ korresponderer til samme tuple(som er ekvivalent med å si at ingen par av kanter har lik vekt og samme starthjørnet). $\hat{T}(C)$ er et Eksempel på en ekte trellis. En trellis T til C sies å være minimal dersom for alle ekte

trelliser $T^{`}$ til $C$ vil $|V_i| \leq |V_i^{`}|$
Vi ser nå på hvordan vi kan konstruere en minimal trellis. Vi begynner med å lage en ekvivalensrelasjon $\sim$ på $\hat{V}_i$ slik: La $t = (a_{i+1}, ..., a_n)$ være en hale til c_i hvis $c_i|t = (a_1, ..., a_i, a_{i+1}, ..., a_n) \in C$. Vi definerer $c_i \sim c_i^{'}$ hvis halemengden til c_i er den samme som til $c_i^{'}$(At $\sim$ oppfyller aksiomene for en ekvivalensrelasjon er lett å se). La $\bar{V}$ være mengden av alle $\bar{V}_i$, der $\bar{V}_i$ er mengden av alle ekvivalensklasser i $\hat{V}_i$. La $\bar{v}_i \in \bar{V}_i$, og $\bar{v}_{i+1} \in \bar{V}_{i+1}$. Da er det en kant fra $\bar{v}_i$ til $\bar{v}_{i+1}$, hvis og bare hvis det finnes hjørner $\hat{v}_i \in \hat{V}_i$ og $\hat{v}_{i+1} \in \hat{V}_{i+1}$, slik at det finnes en kant i T mellom $\hat{v}_i$ og $\hat{v}_{i+1}$, og slik at $\hat{v}_i$ er en representant for ekvivalensklassen $\bar{V}_i$ og $\hat{v}_{i+1}$ er en representant for $\bar{V}_{i+1}$. Videre vil vekten på denne kanten i $\bar{T}$ være den samme som på kanten mellom $\hat{V}_i$ og $\hat{V}_{i+1}$. Dette vil være uavhengig av valg av representanter fra ekvivalensklassene. Trellisen konstruert ovenfor betegner vi $\bar{T}$.

Proposisjon 6.1.1. *$\bar{T}$ er en minimal ekte trellis og alle minimale ekte trelliser er isomorfe til $\bar{T}$.*

Bevis. Se [M] □

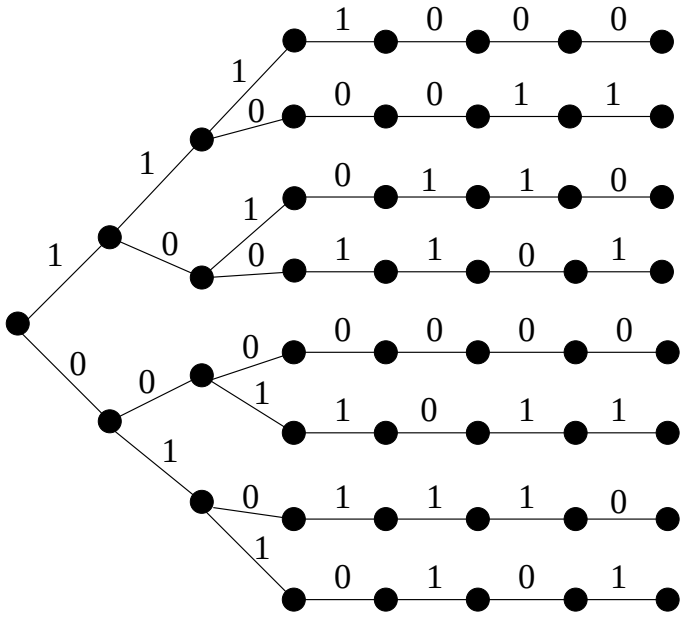
Vi ser nå på hvordan vi kan konstruere minimal trellisen til den duale av $[7, 4, 3]$-Hammingkoden. Se Eksempel 3.28 for en representasjon til generatormatrisen. Ved å permutere 3 og 4 kolonne og 4 og 5 kolonne vil kodeordene være gitt ved:

$$(0,0,0,0,0,0,0),\ (1,1,1,1,0,0,0),\ (1,0,1,0,1,1,0),\ (0,1,1,0,1,0,1)$$
$$(0,1,0,1,1,1,0),\ (1,0,0,1,1,0,1),\ (1,1,0,0,0,1,1),\ (0,0,1,1,0,1,1)$$

En trellis $\hat{T}$ til den duale hammingkoden vil ha åtte kolonner med tilstander. Vi konstruerer en trellis $\hat{T}_i$ til den duale hammingkoden på følgende måte: La de første fire kolonnene bestå av 1, 2, 4 og 8 tilstander, slik at de åtte ulike stiene representerer en unik trippel. La så de neste tre kolonnene bestå av åtte tilstander, slik at de siste fire elementene av hvert kodeord korresponderer til de kant-disjunkte halene. Trellisen $\hat{T}$ til den duale hammingkoden er illustrert i Figur 6.1

Ved å bruke trellisen $\hat{T}$ konstruerer vi minimal trellisen til den duale hammingkoden. De fire første kolonnene må være like for $\bar{T}$ som for $\hat{T}$. Ved å se på de siste tre vektene til hvert kodeord i $\hat{T}$ ser vi at tilstand 1 og tilstand 5 sett ovenfra i kolonne 4 ender med samme trippel(har samme hale av lengde 3). Tilsvarende har vi for tilstand 2 og 6, 3 og 7, 4 og 8. Ved å redusere kolonne 5 til fire tilstander slik at tilstand 1 og 5 i kolonne 4 går mot samme tilstand i kolonne 5 og likeledes for de andre parene av tilstander i kolonne 4 minimerer vi tilstand 5. Videre ser vi at ingen par av vekter er like for de siste to kantlagene i trellisen. Det er derfor ikke mulig å minimere kolonne 6 ytterligere enn 4 tilstander. Kolonne 7 kan reduseres til to tilstander da halvparten av alle kodeord ender med 0 og den andre med 1. Minimal trellisen til den duale hammingkoden er illustrert i Figur 6.2

Enkelte forfattere definerer en trellis ved at den siste kolonnen, V_n, betår av et hjørne(slik at



Figur 6.1: Trellisen $\hat{T}$ til den duale hammingkoden

en trellis alltid er et nettverk). Men uavhengig av hvilken Definisjon vi bruker vil minimal trellisen alltid ha denne egenskapen.

Definisjon 6.1.2. *La $0 \leq i \leq n$. Den foregående underkoden til C er definert ved:*

$$P_i = \{c \in C | c_j = 0 \text{ for alle } j \geq i+1\}$$

Definisjon 6.1.3. *La $0 \leq i \leq n$. Den fremtidige underkoden til C er definert ved:*

$$F_i = \{c \in C | c_j = 0 \text{ for alle } j \leq i\}$$

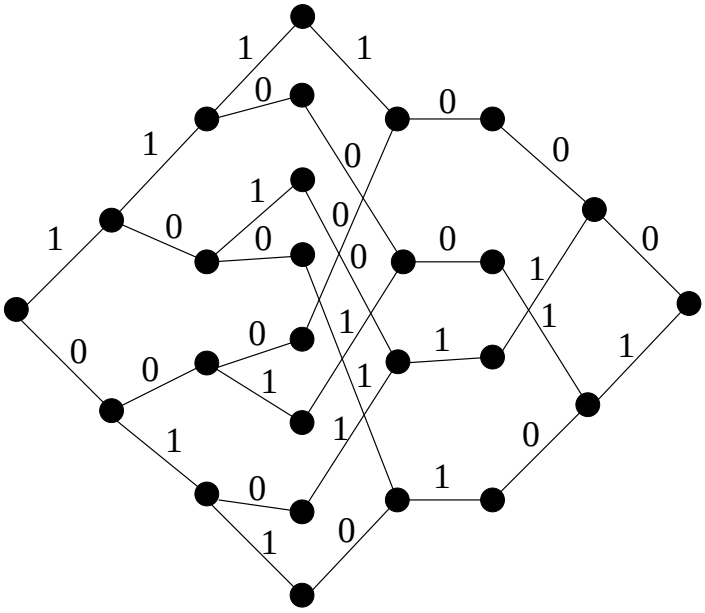
Per konvensjon setter vi $P_n = F_0 = C$. Dersom vi former generatormatrisen, G, til C på trappetrinnform vil F_i utspennes av radene der de ledende 1-erne står til høyre.

Vi gjengir følgende resultat som viser hvordan vi kan finne antall tilstander i en kolonne $\bar{V}_i$ og antall kanter i en kolonne $\bar{E}_{i-1,i}$ til en minimal trellis $\bar{T}$ ved kjennskap til den foregående og fremtidige koden.

Proposisjon 6.1.4. *La $s_i = log_q|\bar{V}_i|$ og la k være dimensjonen til koden. La videre $f_i = dim(F_i)$ og $p_i = dim(P_i)$. Da vil:*

$$s_i = k - p_i - f_i \text{ 1)}$$

$$|\bar{E}_{i-1,i}| = 2^{k-p_{i-1}-f_i} \text{ 2)}$$



Figur 6.2: Trellisen $\bar{T}$ til den duale hammingkoden

Bevis. Vi viser først at $\hat{s}_i = k - f_i$ holder for en generell trellis $\hat{s}_i$. Vi har at $\hat{s}_i = |P_J(C)|$, der $J = \{1, ..., i\}$. La P_J være avbildningen:

$$P_J : C \longrightarrow P_J(C)$$

definert ved:

$$(c_1, ..., c_n) \longrightarrow (c_1, ..., c_i)$$

Kjernen til P_J vil da svare til alle tupleer av lengde n med 0 som koordinat på de i første plassene.

$$kerP_J = \{c|(c_1, ..., c_i) = 0\} = F_i(C)$$

Av "nullitet-rang" Teoremet vil :

$$dimP_J(C) = dimC - dimF_i(C)$$

La $dimP_J(C) = a$. Da vil $|P_J(C)| = q^a$. Vi har da at:

$$\hat{s}_i = log_q|P_J(C)| = log_q q^a = a$$

Derfor vil:

$$\hat{s}_i = dimC - dimF_i(C) = k - f_i$$

Vårt mål er å vise at $\bar{s}_i = k - f_i - p_i$

La Q_J være avbildningen:

$$Q_J : C \longrightarrow F_q^{n-i}$$

Definert ved:

$$(c_1, ..., c_n) \longrightarrow (c_{i+1}, ..., c_n)$$

Vi har tidligere definert halemengde til et forkortet kodeord. Vi har tidligere vist at antall ekvivalensklasser for en trellis $\hat{T}$ er gitt ved q^{k-f_i}, for en gitt tilstand i. Ved å vise at antall elementer i ekvivalensklassene til $(c_1, ..., c_i)$ er q^{p_i} vil dette bevise Proposisjon 6.1.4(Dette vil gi at antall ekvivalensklasser til en minimal trellis er gitt ved $q^{k-f_i}/q^{p_i} = q^{k-f_i-p_i}$).

De mengdene på formen $(d_1, ..., d_i)$ som har samme halemengde som $(0, ..., 0)$(av lengde i) svarer til $P_J(kerQ_J)$. Dette følger av at hvis $(d_1, ..., d_i) \in P_J(kerQ_J)$, da er $(d_1, ..., d_i, 0..., 0)$ et kodeord, og dersom $(d_1, ..., d_i, d_{i+1}, ..., d_n)$ er et kodeord da vil $(0, ..., 0, d_{i+1}, ..., d_n)$ være et kodeord. Dette kodeordet vil da være en hale for $(0, ..., 0)$.
La $(0, ..., 0, c_{i+1}, ..., c_n)$ være et kodeord(dvs en hale til $(0, ..., 0)$), og $(d_1, ..., d_i, 0, ..., 0)$ være et kodeord. Da vil summen av disse kodeordene, $d_1, ..., d_i, c_{i+1}, ..., c_n$, være en hale til $(d_1, ..., d_i)$.

Anta at $(d_1, ..., d_i)$ og $(0, ..., 0)$(av lengde i) har samme halemengde. Da vil summen av disse, $(d_1, ..., d_i, 0..., 0)$, ha $(0, ..., 0)$(av lengde $n - i$) som hale, da $(0, ..., 0)$(av lengde i) har det. Dette gir at $(d_1, ..., d_i) \in P_J(kerQ_J)$.

Vi har vist at 6.1.4 holder for ekvivalensklassen $(0, ..., 0)$. Vi viser nå at den holder for en generell ekvivalensklasse. Hvis $(0, ..., 0)$ og $(d_1, ..., d_i)$ har samme halemengde vil $(a_1, ..., a_i)$ og $(a_1 + d_1, ..., a_i + d_i)$ ha samme halemengde og omvendt.
Dersom $(0, ..., 0)$ og $(d_1, ..., d_i)$ har felles hale $(h_{i+1}, ..., h_n)$ vil differansen, $(d_1, ..., d_i, 0, ..., 0,)$, være et kodeord.

La $(a_1, ..., a_i) \in P_J(C)$. Da vil $(a_1, ..., a_i, h_{i+1}, ..., h_n)$ være et kodeord for passe $(h_{i+1}, ..., h_n)$. Da vil $(a_1 + d_1, ..., a_i + d_i, h_{i+1}, ..., h_n)$ være et kodeord, slik at alle haler også er en hale for $(a_1, ..., a_i)$ og $(a_1 + d_1, ..., a_i + d_i)$. Dersom $(h_{i+1}, ..., h_n)$ er en hale for $(a_1 + d_1, ..., a_i + d_i)$ vil det samme argumentet gi at den også er en hale for $(a_1, ..., a_i)$.

Hvis $(a_1, ..., a_i) \in P_J(C)$ og $(b_1, ..., b_i)$ har samme halemengde vil de ha felles hale $(h_{i+1}, ..., h_n)$. Da vil $(a_1, ..., a_i, h_{i+1}, ..., h_n)$ og $(b_1, ..., b_i, h_{i+1}, ..., h_n)$ være to kodeord. Differansen $(a_1 - b_1, ..., a_i - b_i, 0, ..., 0)$ vil da også vaere et kodeord. Dette gir at $(a_1 - b_1, ..., a_i - b_i) \in P_J(C)$, som videre gir at $(b_1, ..., b_i) = (a_1, ..., a_i) + (a_1 - b_1, ..., a_i - b_i) \in (a_1, ..., a_i) + P_J(kerQ_J)$

La φ være funksjonen P_J avgrenset på kjernen til Q_J. Dvs $\varphi = P_J|_{kerQ_J}$. Av "nullitet-rang" Teoremet har vi at:

$$dim\varphi(kerQ_J) = dimkerQ_J - dimker\varphi$$

Men da vil:

$$ker\varphi = kerP_J|_{kerQ_J} = kerP_J \cap kerQ_J = \{0\}$$

Derfor vil:

$$dimP_J(kerQ_J) = dim\varphi(kerQ_J) = dimkerQ_J = dimP_i(C) = p_i$$

□

Vi illustrerer denne sammenhengen med et eksempel.

Eksempel 6.1.5. *Betrakt den duale hammingkoden med dimensjon lik* 3*. Tabellen under viser* f_i*,* p_i *og* s_i*, der* $0 \leq i \leq 7$

i	0	1	2	3	4	5	6	7
f_i	3	2	1	0	0	0	0	0
p_i	0	0	0	0	1	1	2	3
s_i	0	1	2	3	2	2	1	0

Figur 6.3:

Neste resultat generaliserer Proposisjon 6.1.4:

Teorem 6.1.6. *La* T *være en trellis som representerer en lineær kode* C*. Da vil:*

$$|V_i| \geq 2^{k-p_i-f_i}\text{, for } i = 1, ..., n \text{ 1)}$$

$$|E_{i-1,i}| \geq 2^{k-p_{i-1}-f_i}\text{, for } i = 1, ..., n \text{ 2)}$$

Dersom en av disse ulikhetene er oppfylt med likhet vil begge være oppfylt med likhet og T *vil være isomorf til minimal trellisen* $\bar{T}$

Vi ser nå på hvordan dette har sammenheng med dimensjon/lengde profil. La S_n betegne symmetrigruppen(dvs mengden av alle n-permutasjoner). La $C\pi$ betegne koden C der koordinatene er permutert i henhold til permutasjonen π. Vi har følgende resultat:

Teorem 6.1.7. *La* $k_i(C)$ *være DLP til* C*. La* $p_i(C\pi)$ *betegne dimensjonen til den foregående permuterte koden med hensyn på* π*, og* $f_{n-i}(C\pi)$ *betegne dimensjonen til den fremtidige permuterte koden med hensyn på* π*. Da vil:*

$$k_i(C) = max_{\pi \in S_n} p_i(C\pi) = max_{\pi \in S_n} f_{n-i}(C\pi),\ 1)$$

Bevis. Av Definisjon 4.1.5 har vi at $k_i(C)$ er gitt ved:

$$k_i(C) = max_J\{dim C_J || J| = i\}$$

Underkoden C_J er gitt ved:

$$C_J = \{c | c_i = 0, \text{ når } i \notin J\}$$

Dette betyr at $k_i(C)$ er den maksimale dimensjonen til en underkode $C^{`}$ av $C$ som har støtte(dvs koordinat ulik null) på $i$ plasser. Hvis $C^{`}$ har støtte på i plasser, kan vi lage $C^{`}\pi$ slik at den permuterte underkoden har støtte på de $i$ første plassene. Dvs $p_i(C\pi) = max_{\pi \in S_n} dim(C^{`}\pi)$
Tilsvarende vil $C^{`}\pi$ kunne ha støtte på de siste $i$ plassene(og derfor ikke ha støtte på de første $n - i$ plassene). Derfor vil $f_{n-i}(C\pi) = max_{\pi \in S_n} dim(C^{`}\pi)$. □

Vi har tidligere sett hvordan vi konstruerer en minimal trellis. Vi undersøker nå hvordan vi kan konstruere en minimal trellis for en kode C, slik at trellisen er optimal(i den forstand at antall hjørner er minst mulig), sammenlignet med minimal trellisene for alle permuterte koder $C\pi$. Målet er å gjøre s_i minst mulig. Av Proposisjon 6.1.4 har vi at:

$$min_{\pi \in S_n}(s_i(C\pi)) = k - max_{\pi \in S_n}(p_i(C\pi) + f_i(C\pi))$$

Vi har at:

$$max_{\pi \in S_n}(p_i(C\pi) + f_i(C\pi)) \leq max_{\pi \in S_n} p_i(C\pi) + max_{\pi \in S_n} f_i(C\pi)$$

Som gir:

$$min_{\pi \in S_n}(s_i(C\pi)) \geq k - max_{\pi \in S_n} p_i(C\pi) - max_{\pi \in S_n} f_i(C\pi)$$

Videre har vi da ved 1) at:

$$min_{\pi \in S_n}(s_i(C\pi)) \geq k - k_i - k_{n-i},\ \ 2)$$

Dersom den siste ulikheten er oppfylt med likhet vil dette minimere s_i(dvs antall tilstander i kolonnene til trellisen) og vil i så måte gi opphav til en optimal trellis.

Betrakt en MDS-kode. La generatormatrisen være på formen $k \times n$. Av Definisjonen til en MDS-kode og av Teorem 1.3.20 følger det at alle valg av i kolonner er uavhengige hvis $i \leq k$. Tilsvarende vil alle valg av i kolonner være avhengige hvis $i > k$. Dersom vi permuterer kolonnene til generatormatrisen til en MDS-kode vil den permuterte generatormatrisen generere en MDS-kode. Derfor har vi at C er MDS $\implies C\pi$ er MDS. Av nullitet-rang" Teoremet har vi at:

$$dim C = dim P_J(C) + dim F_i(C)$$

Som gir:

$$dimF_i(C) = dimC - dimP_J(C) = k - min\{i, k\}$$

Vi har derfor at:

$$f_i(C\pi) = k - min\{i, k\}$$

Tilsvarende har vi at:

$$p_i(C\pi) = k - min\{n - i, k\}$$

Vi ser at minimal trellisen til en MDS-kode alltid også vil være en optimal trellis(i den forstand at 2) er oppfylt).

Eksempel 6.1.8. *Vi konstruerer nå en MDS-kode og viser at denne koden oppfyller* 1) *med likhet. La* C *være en* $[4, 2, 3]$*-kode over* F_3*(Denne koden er MDS da* $d = 3 = 4 - 2 + 1 = n - k + 1$*). La* G *være generatormatrisen gitt ved:*

$$\mathbf{G(C)} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

Da C *er MDS vil DLP være gitt ved:* $\{0, 0, 0, 1, 2\}$*. Av* 1) *har vi at:*

$$s_0 \geq k - k_0 - k_4 = 2 - 0 - 2 = 0$$

$$s_1 \geq k - k_1 - k_3 = 2 - 0 - 1 = 1$$

$$s_2 \geq k - k_2 - k_2 = 2 - 0 - 0 = 2$$

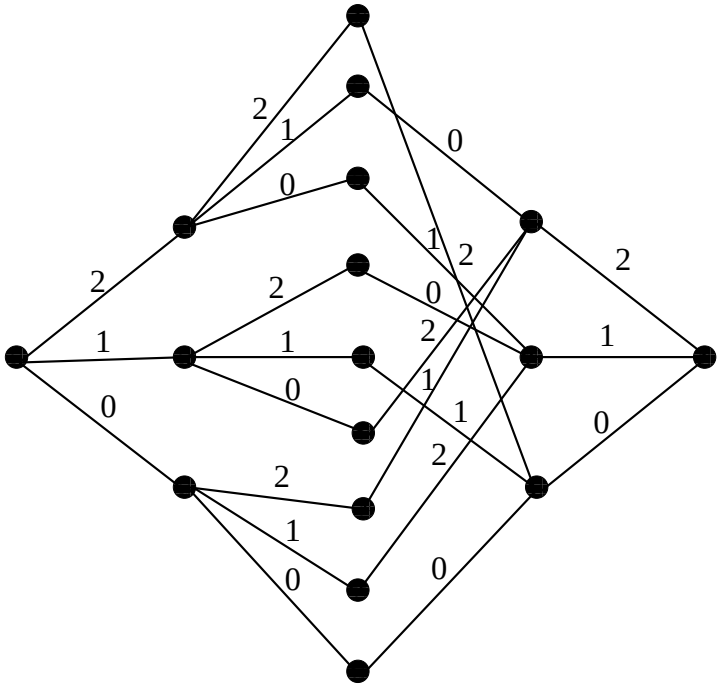
$$s_3 \geq k - k_3 - k_1 = 2 - 1 - 0 = 1$$

$$s_4 \geq k - k_4 - k_0 = 2 - 2 - 0 = 0$$

Ved å liste opp alle kodeordene har vi:

$$(0,0,0,0),\ (1,1,1,0),\ (0,1,2,1),\ (2,2,2,0),\ (0,2,1,2)$$
$$(1,2,0,1),\ (2,0,1,1),\ (1,0,2,2),\ (2,1,0,2)$$

Ved å se på kodeordene er det lett å konstruere en minimal trellis $\bar{T}$*. Vi ser at hvert forkortet kodeord av lengde* 2 *er unikt. Videre ser vi at halene til disse forkortede kodeordene er distinkte. Ved å forene disse halene med de forkortede kodeordene vil de ni stiene i trellisen korrespondere til hver sitt kodeord. Konstruksjonen av trellisen* $\bar{T}$ *er illustrert nedenfor:*



Figur 6.4: Trellisen $\bar{T}$ til $[4, 2, 3]$-koden

Vi har at trellisen består av fem kolonner som hver inneholder henholdsvis 1, 3, 9, 3 *og* 1 *tilstander. Vi ser at vi har klart å konstruere en trellis som oppfyller de nedre begrensningene med likhet. Trellisen* $\bar{T}$ *vil derfor være optimal trellisen til* $[4, 2, 3]$*-koden.*

Vi ser nå på et eksempel hvor ligning 2) ikke er oppfylt med likhet for alle s_i-ene.

Eksempel 6.1.9. *Betrakt dualkoden til* $[7, 4, 3]$*-hammingkoden. DLP er gitt ved:* $\{0, 0, 0, 0, 1, 1, 2, 3\}$. *Av ligning 1) har vi følgende begrensning på* s_i.

$$s_0 \geq k - k_0 - k_7 = 3 - 0 - 3 = 0$$

$$s_1 \geq k - k_1 - k_6 = 3 - 0 - 2 = 1$$

$$s_2 \geq k - k_2 - k_5 = 3 - 0 - 1 = 2$$

$$s_3 \geq k - k_3 - k_4 = 3 - 0 - 1 = 2$$

$$s_4 \geq k - k_4 - k_3 = 3 - 1 - 0 = 2$$

$$s_5 \geq k - k_5 - k_2 = 3 - 1 - 0 = 2$$

$$s_6 \geq k - k_6 - k_1 = 3 - 2 - 0 = 1$$

$$s_7 \geq k - k_7 - k_0 = 3 - 3 - 0 = 0$$

Av Figur 6.2 ser vi at antall tilstander i hver kolonne til minimal trellisen er gitt ved: $1, 2, 4, 8, 4, 4, 2, 1$. *Da vil* s_i *for* $0 \leq i \leq 7$ *være gitt ved:* $0, 1, 2, 3, 2, 2, 1, 0$. *Vi ser at* s_3 *ikke er oppfylt med likhet i ligning 2).*

Vi gir nå et eksempel på to ekvivalente koder som ikke har samme s_i-er(dvs ikke har samme antall tilstander i de tilhørende kolonnene i de respektive trellisene).

Eksempel 6.1.10. *Betrakt den lineære* $[4, 2, 2]$*-koden* C_1 *med generatormatrise gitt ved:*

$$\mathbf{G(C_1)} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Det er lett å se at C_1 *er selvdual. Vi har da at* $S(C_1) = S(C_1^{\perp}) = 4 - 2 - 2 + 1 = 1$. *Da* C_1 *er nær-MDS vil DLP være gitt ved:* $\{0, 0, 1, 1, 2\}$. *Av ligning 1) har vi følgende nedre begrensning på* s_i *for* $0 \leq i \leq 4$.

$$s_0 \geq k - k_0 - k_4 = 2 - 0 - 2 = 0$$

$$s_1 \geq k - k_1 - k_3 = 2 - 0 - 2 = 1$$

$$s_2 \geq k - k_2 - k_2 = 2 - 1 - 1 = 0$$

$$s_3 \geq k - k_3 - k_1 = 2 - 0 - 1 = 1$$

$$s_4 \geq k - k_4 - k_0 = 2 - 2 - 0 = 0$$

Tabellen under viser f_i, p_i *og* s_i *til* C_1 *for* $0 \leq i \leq 4$*:*

Ved å permutere andre og tredje kolonne i $G(C_1)$ *vil generatormatrisen for en ekvivalent kode,* C_2, *til* C_1 *være gitt ved:*

i	0	1	2	3	4
f_i	2	1	0	0	0
p_i	0	0	0	1	2
s_i	0	1	2	1	0

Figur 6.5: Tabellverdiene til C_1

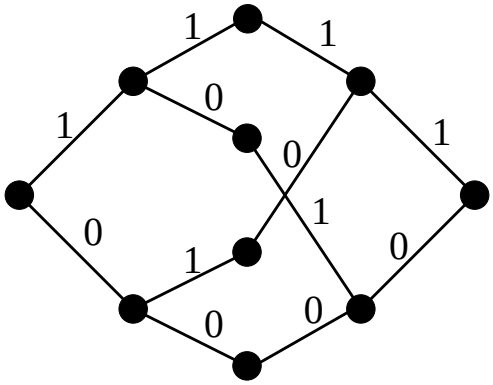
$$\mathbf{G(C_2)} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Tabellen under viser f_i, p_i og s_i til C_2 for $0 \leq i \leq 4$:

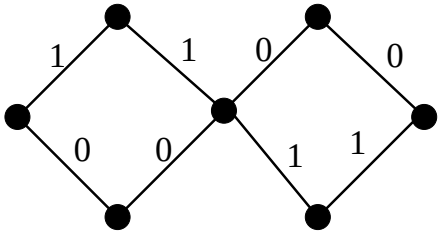
i	0	1	2	3	4
f_i	2	1	1	0	0
p_i	0	0	1	1	2
s_i	0	1	0	1	0

Figur 6.6: Tabellverdiene til C_2

Vi ser at $s_2(C_1) = 2 \neq 0 = s_2(C_2)$. Vi har at minimal trellisen til C_2 er optimal trellisen til C^2, da denne oppfyller 2) med likhet for alle s_i-ene. Nedenfor er trellisene til C_1 og C_2 illustrert.



Figur 6.7: Trellisen til C_1



Figur 6.8: Trellisen til C_2

6.2 Trellisdekoding

For å motivere bruken av trelliser ser vi nå på trellisdekoding. La $\mathbf{y}$ være en motatt vektor fra sender. Denne vektoren trenger ikke være et kodeord da støy på kanalen kan ha forårsaket at en eller flere feil har oppstått under sending. Vi skal å se på en algoritme, Viterbialgoritmen, som finner stien(dvs kodeordet) med minst Hammingavstand fra det motatte kodeordet. Vi formulerer Viterbialgoritmen i tre steg:

1) For hver i og hvert hjørne i kolonne i finn Hammingavstanden mellom i-trunkeringen av det motatte kodeordet og alle stiene fra kilden til hjørnet i kolonne i, rekursivt ved hjelp av nivå $i-1$.

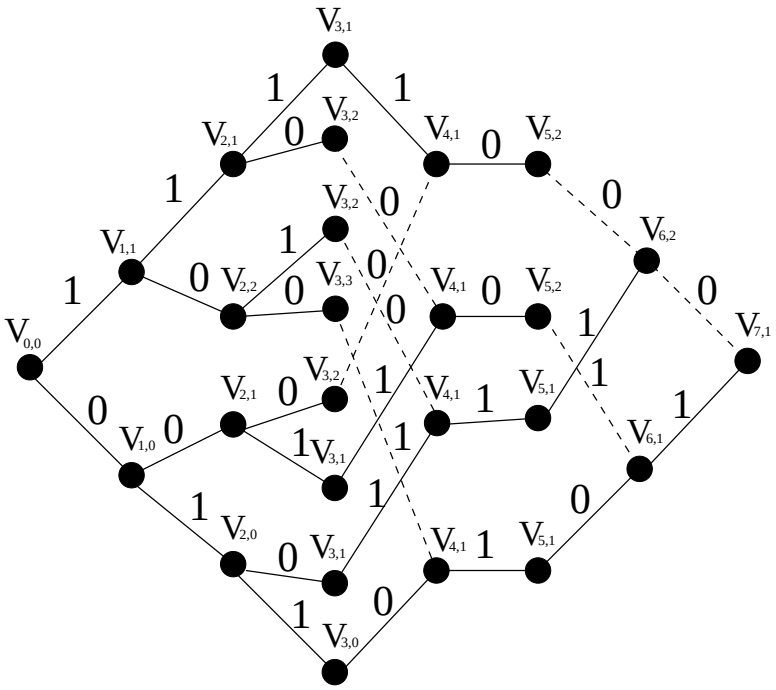
2) For hvert hjørne, stryk stiene som ikke gir minimum Hamming avstand.

3) Gjenta steg 1) og 2) for kolonne $i+1$

Vi illusterer algoritmen ved å gjennomgå stegene i et Eksempel.

Eksempel 6.2.1. *Betrakt minimal trellisen, $\bar{T}$, til $[7,3,4]$-Hammingkoden som vi tidligere har konstruert. Denne koden er 1-feil korrigerende. Gitt at vi mottar vektoren $\boldsymbol{y} = 0111101$.*

Vi dekoder nå $\mathbf{y}$ *ved å følge stegene i Viterbialgoritmen. Vi kan bare stryke kanter dersom det går flere kanter inn mot hjørnet. Derfor kan vi ikke stryke noen kanter i de tre første kolonnene av kanter, heller ikke i kolonne* 5. *I kolonne* 4,6 *og* 7 *stryker vi de kantene som ikke gir minimalverdi. Vi traverserer så baklengs i trellisen fra målet til kilden, og finner da det kodeordet som er nærmest* $\mathbf{y}$. *Stegene i algoritmen er illustrert i trellisen nedenfor. Vi markerer kantene som strykes med en stiplet linje. For hver tilstand i trellisen setter vi en verdi* $V_{i,j}$, *der i betegner kolonnen med hjørner og j betegner hammingavstanden mellom i-trunkeringen av den motatte vektoren og stien fra kilden til hjørnet i kolonne i. Av figuren under ser vi at den eneste stien(kodeordet) som er igjen er den vi får ved å følge de nederste kantene i trellisen.*



Figur 6.9: Illustrasjon av Viterbialgoritmen

Vi ser av Eksempelet at Viterbialgoritmen reduserer antall sammenligninger vi må gjøre for å dekode den motatte vektoren til det korrekte kodeordet. I informatiske termer kan vi si at kompleksiteten(et mål for hvor mye ressurser(tid og plass) som trengs for å løse et problem algoritmisk) reduseres ved bruk av Viterbialgoritmen. Kompleksiteten samsvarer med antall tilstander i trellisen. Jo mindre trellisen er desto mindre er kompleksiteten. I de ytterligående tilfellene, vil den trivielle trellisen(den vi får ved å la kodeordene være representert av kant-disjunkte stier) svare til at vi finner Hammingavstanden mellom det

motatte kodeordet og alle kodeordene i koden, og vil derfor ikke redusere kompleksiteten. Tilsvarende vil kompleksiteten være mest mulig redusert ved bruk av minimal trellis(minst mulig sammenligninger er nødvendig).

Bibliografi

[C] P. J. Cameron, *Codes, matroids and trellises*, 15 siders preprint (2000), link tilgjengelig på http://www.maths.qmul.ac.uk/∼pjc/papers.html.

[F] G.D [Forney], *Dimension/Length Profiles and Trellises Coplexity of Linear Block Codes*, IEEE Trans. on Information Theory, Vol 40, No 6, s 1741-1745, 1994.

[H] R [Hill], *A First Course in Coding Theory*, Oxford University Press, Oxford, 1986.

[LMVC] Y. Luo, C. Mitrpant, *Some New Characters on the Wire-Tap Channel of Type 2*, IEEE Trans. on Information Theory, Vol 42, No 4, s 1222-1227, 2005.

[McE] R.J. [McEliece], *On the BCJR Trellis for Linear Block Codes*, IEEE Trans. on Information Theory, Vol 51, No 3, s 1080-1082, 2005.

[L] A.H. Larsen, *Matroider og lineære koder*, hovedfagsoppgave, Universitetet i Bergen, 2005.

[M] D.J. [Muder], *Minimal Trellises for Block Codes*, IEEE Trans. on Information Theory, Vol 34, No 5, s 1049-1053, 1988.

[O] J. [Oxley], *Matroid theory*, Oxford University Press, Oxford, 1992.

[R] H. Raddum, *MDS-formodningen og vekthierarkiet for sterkt algebraisk-geometriske koder*, hovedfagsoppgave, Universitetet i Bergen, 1999.

[TW] W. Trappe, L.C. Washington *Introduction to Cryptography with Coding Theory*, Prentice Hall, Upper Saddle River, New Jersey, 2002.

[Wei] W V. [Wei], *Generalized Hamming [Wei]ghts for Linear Codes*, IEEE Trans. on Information Theory, Vol 37, No 5, s 1412-1418, 1991.

[Wel] D.J.A. [Welsh], *Matroid theory*, Academic Press, London, 1976.

[Wil] R.J. Wilson, *Introduction to Graph Theory*, Longman, Harlow, 1996.